BayRS Version 14.20

Part No. 308625-14.20 Rev 00
October 2000

600 Technology Park Drive
Billerica, MA 01821-4130

Configuring GRE, NAT, RIPSO, and BFE Services

NORTEL NETWORKS™

Copyright © 2000 Nortel Networks

All rights reserved. October 2000.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

BCN and BLN are registered trademarks and ASN, BCC, BayRS, and BayStack are trademarks of Nortel Networks.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks NA Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License grant. Nortel Networks NA Inc. ("Nortel Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible

for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Text Conventions xvi
Acronyms xvii
Related Publications xviii
How to Get Help xix

Chapter 1
Configuring GRE Tunnels

GRE Concepts and Terminology 1-2
How GRE Tunneling Works 1-3
Example of Packet Handling in a GRE Tunnel 1-4
GRE Packet Headers 1-5
Requirements for GRE Tunnels Encapsulating IP Protocol 1-7
Announce Policies 1-7
Accept Policies 1-8
Static Routes 1-8
Number of Tunnels Configurable per Router 1-9
For IP and IPX 1-9
For OSI 1-9
Creating a GRE Tunnel 1-10
Configuring the Local Tunnel End Point 1-10
Adding a Protocol to the Local Tunnel End Point 1-12
Adding an IP Protocol Interface 1-12
Adding an IPX Protocol Interface 1-13
Adding an IP or an IPX Protocol Interface 1-13
Adding an OSI Protocol Interface 1-14
Configuring the Remote Tunnel End Point 1-16

Using the BCC 1-17
Step 1. Configuring a Remote Physical Interface 1-17
Step 2. Configuring a Remote Logical Interface 1-17
Using Site Manager 1-19
Configuring a Remote End Point for IP or IPX 1-19
Configuring a Remote End Point for OSI 1-20
Customizing a GRE Tunnel 1-21
Disabling and Reenabling a GRE Tunnel 1-21
Disabling and Reenabling a Protocol on a GRE Tunnel 1-22
Deleting a Protocol from a GRE Tunnel 1-24
Disabling and Reenabling a Remote Tunnel End Point 1-25
Deleting a Remote Tunnel End Point 1-26
Deleting a GRE Tunnel 1-27

Chapter 2
Configuring Network Address Translation

NAT Concepts 2-2
Unidirectional NAT 2-3
Advantages 2-3
Requirements 2-4
For More Information About Unidirectional NAT 2-4
Representing Multiple Hosts with a Single Address: SDPT and N-to-1 2-5
For More Information on SDPT and N-to-1 2-6
Bidirectional (Multidomain) NAT 2-7
Advantages 2-7
Requirements 2-7
How DNS Server, DNS Client, and DNS Proxy Work with Bidirectional NAT 2-8
For More Information on Bidirectional NAT 2-9
Translation Modes 2-10
Static Translation Mode 2-10
Dynamic Translation Mode 2-11
Examining How Different Types of NAT Work 2-13
Unidirectional NAT 2-14
Static Unidirectional Address Translation 2-14
Dynamic Unidirectional Address Translation 2-15

Static Destination and Port Translation (SDPT) 2-20
Network Address Port Translation (N-to-1) 2-23
Bidirectional NAT 2-26
Static Bidirectional Address Translation 2-26
Dynamic Bidirectional Address Translation with Two Domains 2-28
Dynamic Bidirectional Address Translation with Three Domains 2-29
NAT Implementation Guidelines 2-32
NAT General Configuration Considerations 2-32
Protocol Requirements and Compatibilities 2-33
NAT Requires IP Forwarding 2-33
OSPF and BGP Supported for Unidirectional NAT Only 2-33
ISP Mode Not Supported by NAT 2-33
ECMP Mode Supported for Unidirectional NAT Only 2-33
Compatibility of NAT and IPsec on a Router Interface 2-34
Special Considerations for Configuring NAT SDPT for FTP 2-34
Special Considerations for Configuring NAT SDPT for TFTP 2-34
Multiple Source Address Filters -- Order of Precedence for NAT Types 2-35
Internet Control Message Protocol and Message Handling 2-39
Starting NAT Services and Configuring Translations 2-40
Configuring Unidirectional NAT (Dynamic) 2-40
Using the BCC 2-40
Using Site Manager 2-45
Configuring Bidirectional NAT (Dynamic) 2-50
Using the BCC 2-50
Using Site Manager 2-56
Where to Go Next 2-64
Customizing NAT Global Parameters 2-65
Enabling and Disabling NAT on the Router 2-66
Configuring the Soloist Slot Mask 2-67
Logging NAT Messages 2-69
Enabling and Disabling the Dynamic Mapping Aging Timer 2-71
Configuring the Dynamic Mapping Timeout Value 2-72

Customizing a NAT Interface 2-74
Adding NAT to an Interface 2-74
Disabling and Reenabling NAT on an Interface 2-77
Deleting NAT from an Interface 2-79
Configuring NAT Static Address Translation 2-80
Adding a Static Unidirectional Address Mapping 2-81
Adding a Static Bidirectional Address Mapping 2-84
Examples of Configuring Static Bidirectional NAT to Work with or Independent of DNS Proxy on the NAT Router 2-87
Adding an SDPT Address and Port Mapping 2-89
Disabling and Reenabling a Static Address Mapping 2-92
Deleting a Static Address Mapping 2-93
Configuring NAT Dynamic Address Translation 2-95
Adding a Source Address Filter 2-97
IP Address and Prefix Length Parameter 2-98
Domain Name Parameter 2-98
Translation Pool Parameter 2-98
Static Nexthop Address Parameter 2-99
Unnumbered Circuit Name Parameter 2-99
Disabling and Reenabling a Source Address Filter 2-103
Deleting a Source Address Filter 2-105
Adding a Translation Pool 2-106
Disabling and Reenabling a Translation Pool 2-109
Deleting a Translation Pool 2-111
Configuring NAT N-to-1 Translation 2-113

Chapter 3
Configuring RIPSO on an IP Interface

RIPSO Concepts and Terminology 3-2
Security Label Format 3-3
Inbound IP Datagrams 3-4
Forwarded IP Datagrams 3-5
Originated IP Datagrams 3-5
Unlabeled IP Datagrams 3-5
Enabling and Disabling RIPSO 3-6
Specifying the IP Datagram Type for Stripping Security Options 3-7

Specifying the Outbound Datagram Type Requiring Security Labels 3-8
Specifying the Inbound Datagram Type Requiring Security Labels 3-9
Setting the Security Level for IP Datagrams 3-10
Choosing Authority Flags in Outbound Datagrams 3-11
Choosing Authority Flags in Inbound Datagrams 3-12
Supplying Implicit Labels for Unlabeled Inbound Datagrams 3-13
Enabling and Disabling Default Labels for Unlabeled Outbound Datagrams 3-14
Enabling and Disabling Error Labels for Outbound ICMP Error Datagrams 3-15
RIPSO Example 3-16

Chapter 4
Connecting the Router to a Blacker Front End

Blacker Front End (BFE) Concepts and Terminology 4-2
BFE Addressing 4-4
Configuring BFE Support 4-5

Appendix A
Site Manager Parameters

GRE Parameters A-2
GRE Tunnel Parameters A-2
Remote Connection Parameters A-4
NAT Parameters A-7
NAT Global Parameters A-7
NAT Interface Parameters A-11
NAT Static Translation Parameters A-12
Adding Static Translation Parameters A-16
NAT Dynamic Mapping Parameters A-24
NAT Source Address Filter Parameters A-25
Adding Source Address Filter Parameters A-28
NAT Translation Pool Parameters A-31
Adding NAT Translation Pool Parameters A-32
RIPSO Parameters A-34

Appendix B
Sample Bidirectional NAT Configuration

Overview of Configuration Tasks B-1
Sample Scenario B-2

Configuring Sample Bidirectional NAT Using the BCC B-3
Information Used in Bidirectional NAT Configuration B-3
Checking Address Translations B-10
show nat domains (BCC) B-11
show nat mappings (BCC) B-12
show nat translations (Technician Interface) B-13

Index

Figures

Figure 1-1. Simple GRE Tunnel Components 1-3
Figure 1-2. GRE Tunnel Encapsulating the IP Protocol 1-5
Figure 1-3. GRE Packet Headers 1-6
Figure 1-4. Detail of GRE Header 1-6
Figure 2-1. Static Unidirectional NAT Configuration 2-14
Figure 2-2. Network Address Translation Example 2-16
Figure 2-3. NAT Detects the Source Address 2-17
Figure 2-4. NAT Updates the Private/Public Translation Entry List 2-18
Figure 2-5. NAT Replaces the Private Address with a Registered Source Address 2-19
Figure 2-6. Sample Configuration for NAT SDPT 2-21
Figure 2-7. N-to-1 Translation (Part 1) 2-24
Figure 2-8. N-to-1 Translation (Part 2) 2-25
Figure 2-9. Static Bidirectional NAT Configuration 2-26
Figure 2-10. Bidirectional NAT with DNS Proxy 2-28
Figure 2-11. Bidirectional NAT with Three Domains 2-30
Figure 2-12. Network Address Translations Associated with Figure 2-11 2-31
Figure 2-13. Sample Translation Types and Address Ranges 2-36
Figure 2-14. More Sample Translation Types and Address Ranges 2-37
Figure 2-15. Non-overlapping Address Ranges 2-38
Figure 3-1. RIPSO Security Label 3-3
Figure 3-2. RIPSO Example 3-17
Figure 4-1. BFE Network Configuration 4-2
Figure A-1. GRE Create Tunnels List Window A-2
Figure A-2. Create GRE Remote Connection Window A-4
Figure A-3. IP Interface List Window A-34
Figure B-1. Sample Configuration for Bidirectional NAT B-2

Tables

Table 2-1. Comparing NAT Types SDPT and N-to-1 2-5
Table 2-2. Sample Configuration for a Router Configured with NAT 2-22
Table 2-3. NAT Log Message Types 2-69
Table 4-1. BFE X.25 Packet-Level Parameter Settings 4-6
Table 4-2. BFE X.25 Network Service Record Parameter Settings 4-8
Table B-1. Information to Gather Before Configuring NAT B-3
Table B-2. Available show nat Commands B-10

Preface

This guide describes the following services and what you do to start and customize them on a Nortel Networks™ router:

- Generic Routing Encapsulation (GRE) tunnels
- Network Address Translation (NAT)
- Basic Revised IP Security Option (RIPSO) security labels
- Blacker front-end (BFE) device connections

You can use Site Manager to configure any of these services on a router. You can also use the Bay Command Console (BCC™) to configure GRE and NAT. In this guide, you will find instructions for using both the BCC and Site Manager.

For instructions on how to start and use the BCC, see *Using the Bay Command Console (BCC)*; for instructions on how to start and use Site Manager, see *Configuring and Managing Routers with Site Manager.*

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Nortel Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** <*ip_address*>, you enter: **ping 192.32.10.12**
bold text	Indicates command names and options and text that you need to enter. Example: Enter **show ip** {**alerts** | **routes**}. Example: Use the **dinfo** command.
braces ({ })	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you must enter either: **show ip alerts** or **show ip routes**, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is: **show ip interfaces** [**-alerts**], you can enter either: **show ip interfaces** or **show ip interfaces -alerts**.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.

`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

This guide uses the following acronyms::

ACC	access control center
BFE	Blacker front end
BCN	Backbone Concentrator Node
BGP	Border Gateway Protocol
BLN	Backbone Link Node
DCE	data communication equipment
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPX	Internetwork Packet Exchange

ITU-T	International Telecommunication Union-Telecommunication Standardization Sector (formerly CCITT)
KDC	key distribution center
MAC	media access control
NAT	Network Address Translation or Network Address Translator
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
RIPSO	Revised IP Security Option
SAP	Service Advertising Protocol
SDPT	Static Destination and Port Translation
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VPN	virtual private network
WAN	wide area network

Related Publications

For more information about GRE, NAT, and other IP services, refer to the following publications:

- *Reference for BCC IP show commands*
  (Nortel Networks part number 308603-14.00 Rev 00)

  Provides descriptions of all **show** commands for IP services, including the commands that display GRE and NAT configuration and statistical data.

- *Configuring IP, ARP, RARP, RIP, and OSPF Services*
  (Nortel Networks part number 308627-14.00 Rev 00)

  Provides a description of IP, ARP, RARP, RIP, and OSPF services and instructions for configuring them.

- *Configuring IP Exterior Gateway Protocols (BGP and EGP)*
  (Nortel Networks part number 308628-14.00 Rev 00)

  Provides a description of Border Gateway Protocol (BGP) and Exterior Gateway Protocol (EGP) services and instructions for configuring them.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the support.baynetworks.com/library/tpubs/ URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Acrobat Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at www.adobe.com to download a free copy of Acrobat Reader.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

How to Get Help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
EMEA	(33) (4) 92-966-968
North America	(800) 2LANWAN or (800) 252-6926
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.

Chapter 1
Configuring GRE Tunnels

This chapter provides information about Generic Routing Encapsulation (GRE) tunnels and instructions for configuring them. It includes the following sections:

Topic	Page
GRE Concepts and Terminology	1-2
Creating a GRE Tunnel	1-10
Customizing a GRE Tunnel	1-21
Deleting a GRE Tunnel	1-27

GRE Concepts and Terminology

Generic Routing Encapsulation (GRE) is a protocol that allows transport of non-IP traffic through IP-based systems. GRE, which is defined in RFCs 1701 and 1702, encapsulates Internet Protocol (IP) and other layer 3 protocols to enable data transmission through an IP tunnel. This tunneling mechanism allows:

- Transport of non-IP traffic through intermediate systems that support only IP
- Creation of a virtual private network (VPN) that uses the Internet as a section of your own private network
- Communication between subnetworks with unregistered or discontiguous network addresses

A *tunnel* is a virtual point-to-point connection. It has as its end points the IP addresses of two router IP interfaces, one serving as the source, the other serving as the destination. When using GRE, remember that:

- This protocol is slower than native routing because packets require additional processing.
- IP fragmentation of the packet can occur due to extra bytes introduced by encapsulation.
- Troubleshooting the physical link when problems occur is difficult.

GRE tunnels support encapsulation of the following protocols:

- IP - Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP)
- Internet Protocol Exchange (IPX) and IPX RIP/Service Advertising Protocol (SAP)
- Open Systems Interconnection (OSI)

How GRE Tunneling Works

A simple point-to-point GRE tunnel terminates at router interfaces at each end of the tunnel (Figure 1-1). Each interface has a physical address and may have one or more logical addresses. For IP and IPX protocols, at each tunnel end point there is one logical address for each protocol configured for encapsulation over the tunnel. Because the concept of an interface address does not exist in OSI, only one IP address is required per router.

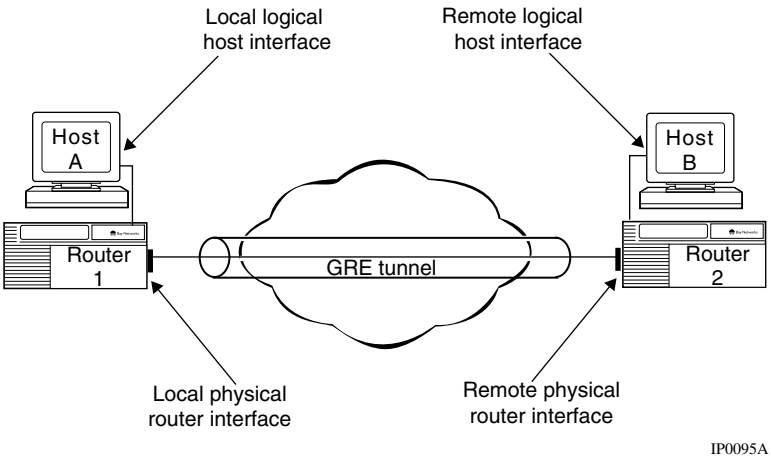


Figure 1-1. Simple GRE Tunnel Components

The physical address, which is always an IP address, is visible to the devices making up the intervening network cloud. The logical addresses are *not* visible to the devices that make up the intervening network cloud. They are private addresses, visible only to the networks on either side of the tunnel.

The GRE tunnel can use any IP interface configured on the router as a physical end point. To maximize the robustness of the tunnel, use a circuitless IP address as a tunnel's physical end point whenever possible. Because a circuitless IP address is associated with the whole router, not one physical interface, the tunnel operates as long as any slot that has a working IP interface stays up. (For instructions on configuring a circuitless interface, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.)

Example of Packet Handling in a GRE Tunnel

The following steps explain how GRE tunneling takes place. The example describes a GRE tunnel encapsulating IP or IPX (refer to Figure 1-2).

1. The router interface on router 1 receives a packet from host 1, looks up the packet's destination address in its IP routing table, and determines that the next hop to the destination address is the remote end of a GRE tunnel. The router interface queues the packet at the tunnel interface for GRE encapsulation.
2. Router 1 adds a GRE header to the packet and sends the packet to IP.
3. IP looks up the route to the remote tunnel end point and sends the GRE-encapsulated packet to the appropriate next-hop address.
4. The remote tunnel interface on router 2 removes the outer IP header and the GRE header.
5. The remote router interface looks up the packet's destination address in its routing table and chooses the next hop to reach host 2.

The same process would take place for IPX.

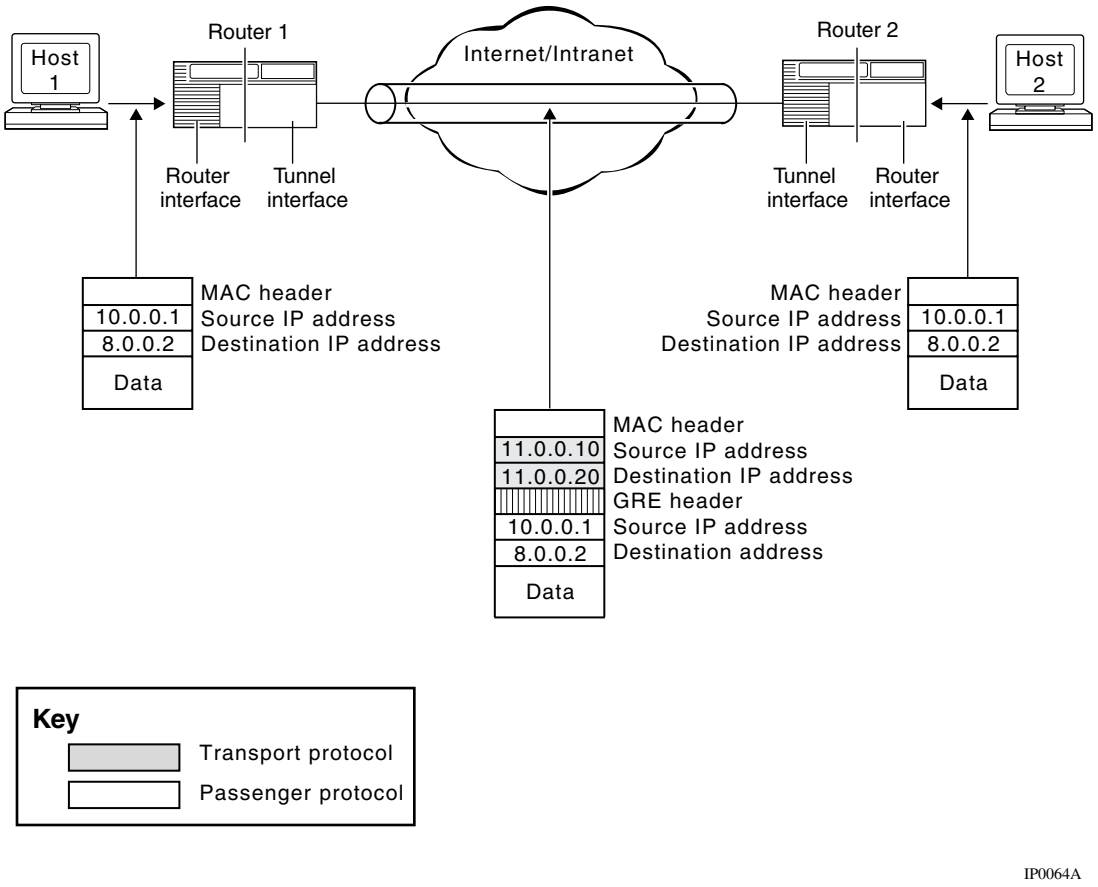


Figure 1-2. GRE Tunnel Encapsulating the IP Protocol

GRE Packet Headers

The previous example followed the path of a GRE packet as it traversed the tunnel, explaining its handling. Here is some detail about what occurs with the headers of such a GRE packet. A GRE packet has the following headers (Figure 1-3):

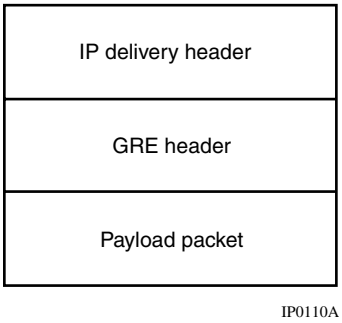


Figure 1-3. GRE Packet Headers

The outermost (delivery) header is an IP header with protocol type 0x47 (GRE). For a packet arriving at the router through a tunnel, the destination address is an IP interface that the network administrator configures as the GRE tunnel remote end point. The next header is the GRE header (Figure 1-4). The last header is the payload. The payload could be IP, IPX, or OSI, in which case it would contain an identifying header of the protocol type.

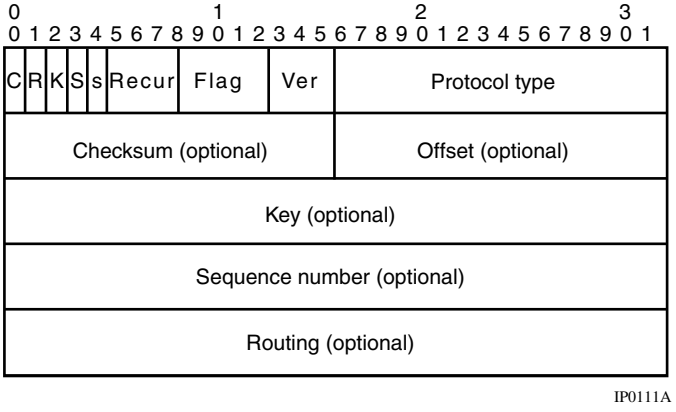

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
C R K S s Recur
Flag
Ver
Protocol type
Checksum (optional)
Offset (optional)
Key (optional)
Sequence number (optional)
Routing (optional)
IP0111A

Figure 1-4. Detail of GRE Header

For a more complete description of the GRE header, see RFC 1701.

Requirements for GRE Tunnels Encapsulating IP Protocol

Note: If you are using GRE tunneling to encapsulate the IPX or OSI protocol, skip this section. The requirements discussed below *do not* apply to tunnels encapsulating IPX or OSI.

Before configuring a tunnel encapsulating IP, you should be aware of a limitation inherent in the use of all tunnels, including GRE tunnels. A tunnel is a virtual point-to-point connection between two routers that are actually several hops apart. This point-to-point connection can hide the real distance between the routers from portions of the network, leading to unintended, suboptimal routing decisions and in some cases, to routing loops.

In particular, if a router at one end of a tunnel determines that the best route to the remote physical end point of the tunnel is through the tunnel itself, a loop, internal to the router, occurs and prevents the tunnel from operating. You must configure one of the following at each end of the tunnel to prevent routing loops:

- Announce policy
- Accept policy
- Static route

The best choice depends on the network topology to which it is applied.

Note: When configuring a tunnel with IP encapsulation, you must implement an announce or accept policy or a static route at each end of the tunnel for the tunnel to operate correctly.

Announce Policies

An *announce policy* governs the advertisement of routing information. When preparing a routing advertisement, IP consults its announce policies to determine whether to advertise the route. For GRE tunneling, you can configure an announce policy for each routing protocol (RIP, OSPF, BGP) configured on the logical tunnel interface to block the advertisement of a range of network addresses that contains the tunnel's local physical interface address. For information about configuring RIP and OSPF announce policies, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*. For information about configuring BGP announce policies, see *Configuring IP Exterior Gateway Protocols (BGP and EGP)*.

The disadvantage of using an announce policy is that it prevents the advertisement of other subnets within the blocked range. Depending on the network topology, this configuration may not be desirable.

Accept Policies

An *accept policy* governs the addition of new routes to the routing tables. For GRE tunneling, you can configure an accept policy for each routing protocol (RIP, OSPF, BGP) configured on the logical tunnel interface to block the receipt of advertisements from a range of network addresses that contains the tunnel's remote physical interface address. For information about configuring RIP and OSPF accept policies, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*. For information about configuring BGP accept policies, see *Configuring IP Exterior Gateway Protocols (BGP and EGP)*.

The disadvantage of using an accept policy is that it prevents the receipt of advertisements of subnets contained in the blocked range. Depending on the network topology, this configuration may not be desirable.

Static Routes

A *static route* is a route configuration that designates a specific router within the intervening network cloud as the next hop to the remote physical tunnel end point. Because static routes take precedence over routes that the router learns dynamically from routing protocols, this configuration forces the router to direct packets through the cloud to reach the tunnel's remote physical address.

The disadvantage of using a static route is that it is fixed. If the path through the chosen next hop to the remote tunnel end point goes down, the tunnel goes down as well until you manually reconfigure the static route. Similarly, even if the path through the chosen next hop becomes more costly than the path through some other attached router, the tunnel continues to use the more costly path unless you manually intervene.

Note: When configuring a static route, be careful not to inadvertently create a loop.

Number of Tunnels Configurable per Router

The number of GRE tunnels you can configure on a router varies, depending on the type of protocol being encapsulated.

For IP and IPX

You can create up to 64 GRE tunnels on one router; each GRE tunnel can have multiple end points. You can configure up to 256 remote tunnel end points distributed over the configured GRE tunnels for IP and IPX.

For OSI

GRE point-to-point and point-to-multipoint tunnels are viewed by OSI as point-to-point subnetworks as defined by ISO 10589. Each GRE tunnel appears as a single OSI interface. Configure GRE tunnels for OSI traffic within the following guidelines:

- Each router interface can support one GRE tunnel configured with OSI.
- A single 32 Mb router slot can support a maximum of 48 interfaces.
- The maximum number of end points per tunnel is 150.

Theoretically, a single slot could support 48 interfaces, each of which could be a point-to-multipoint configuration. OSI would treat this configuration as 48 groups of point-to-point subnetworks with each subnetwork having an adjacency. (An *adjacent* router is the next hop on the path toward the destination.) Each adjacency would have its own state machine, and flooding of data would be resource intensive because datagrams would need to be propagated along each adjacency. Such a configuration would have implications for buffer and memory usage.

Creating a GRE Tunnel

To create a tunnel:

1. **Configure the local tunnel end point.**
2. **Add one or more protocols (IP, IPX, or OSI) to the local tunnel end point.**
3. **Configure the remote tunnel end point.**

For instructions, see:

Topic	Page
Configuring the Local Tunnel End Point	1-10
Adding a Protocol to the Local Tunnel End Point	1-12
Configuring the Remote Tunnel End Point	1-16

Configuring the Local Tunnel End Point

When you create a GRE tunnel, you assign the tunnel a name and an IP address. The IP address is the router interface used as the local physical end point for this tunnel. The IP address must be that of an existing physical router IP interface or the circuitless address. To maximize the robustness of the tunnel, use a circuitless IP address as a tunnel's physical end point whenever possible. (For instructions on configuring a circuitless IP interface, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.)

This IP address is visible to the network cloud that the tunnel passes through.

Using the BCC

To configure the local tunnel end point of a GRE tunnel:

1. **Navigate to the box or stack prompt and enter:**

   tunnels

   The tunnels prompt appears.

2. **Navigate to the tunnels prompt (for example, box; tunnels) and enter the following command:**

   gre name *<name>* **local-address** *<address>*

name is a unique name for this tunnel.

address is a valid IP address of a local router interface expressed in dotted-decimal notation.

For example, the following command sequence creates the tunnel *boston* with the local physical end point 197.1.2.3 and verifies the addition:

```
tunnels# gre name boston local-address 197.1.2.3
gre/boston# info
    local-address 197.1.2.3
    name boston
    state enabled
```

Using Site Manager

To configure the local tunnel end point of a GRE tunnel, first configure IP on an interface, and then complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Click on **Add Tunnel**.	The Create GRE Tunnel window opens.
5. Set the following parameters: • **IP Interface** • **Tunnel Name** Click on **Help** or see the parameter descriptions beginning on page A-3.	
6. Click on **OK**.	You return to the GRE Create Tunnels List window.

Adding a Protocol to the Local Tunnel End Point

The Nortel Networks implementation of GRE tunneling supports the encapsulation of the IP, IPX, and OSI protocols over a GRE tunnel. When you add a protocol to a tunnel, you are configuring its local logical interface. The local logical interface is the address of the local host, the tunnel's local logical end point. This address is not visible to the network cloud that the tunnel passes through.

Note: You can configure OSPF on either a GRE tunnel's physical interfaces or its logical interfaces, but not on both. When configuring OSPF on a GRE tunnel, disable MTU mismatch detection. If the MTU mismatch parameter is enabled, an OSPF adjacency may fail to form over the tunnel.

Using the BCC

You can use the BCC to add an IP or an IPX protocol interface to a GRE tunnel.

Adding an IP Protocol Interface

To add an IP protocol interface to the local tunnel end point, navigate to the GRE tunnel interface prompt (for example, **box; tunnels; gre/boston**) and enter:

ip address *<address>* **mask** *<address>*

address is the valid IP address of the host interface at the local end of the tunnel expressed in dotted-decimal notation.

mask is the mask associated with the IP address.

For example, the following command adds the IP interface 9.9.9.1/255.255.255.0 to the tunnel *boston*:

```
gre/boston# ip address 9.9.9.1 mask 255.255.255.0
ip/9.9.9.1/255.255.255.0#
```

For a complete description of IP interface configuration, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

To configure an IPX protocol interface, go to the next section. Otherwise, go to "Configuring the Remote Tunnel End Point" on page 1-16.

Adding an IPX Protocol Interface

To add an IPX protocol interface to the local tunnel end point, navigate to the GRE tunnel interface prompt (for example, **box; tunnels; gre/boston**) and enter:

ipx address *<address>* **host-address** *<host_address>*

address is a valid IPX network ID. Enter a four-byte hexadecimal string of up to eight characters.

host_address is a valid IPX host address that is unique within the IPX internetwork. Enter up to four characters in hexadecimal format. The IPX host address maps to a physical data link layer address on a specific circuit or physical interface.

For example, the following command adds the IPX interface 00112233 with the host address 4411 to the tunnel *boston*:

```
gre/boston# ipx address 00112233 host-address 4411
ipx/00112233#
```

For a complete description of IPX interface configuration, see *Configuring IPX Services*.

Using Site Manager

The steps to add a protocol to the local tunnel end point vary, depending on which protocol you are assigning.

Adding an IP or an IPX Protocol Interface

To add an IP or an IPX protocol to the local tunnel end point, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose a tunnel from the list, and then click on **Add/Del Prot**.	The Select Protocols window opens.
5. Choose one or more protocols from the list, and then click on **OK**.	The appropriate protocol configuration windows open.
6. Enter the required information to configure the IP or IPX interface, then click on **OK**. For information about any parameter, click on **Help** or see the appropriate protocol guide.	You return to the GRE Create Tunnels List window.
7. Click on **Done**.	You return to the Configuration Manager window.

Adding an OSI Protocol Interface

To add the OSI protocol to the local tunnel end point, complete the following tasks. These instructions assume that one or more GRE tunnels have already been configured.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Choose a tunnel from the list, and then click on **Add/Del Prot**.	The Select Protocols window opens.
5. Choose OSI from the list, and then click on **OK**.	The OSI Configuration window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Set the following parameters (required if OSI has not been configured previously on any other router interface): • **Router ID (hex)** • **Area Address (hex)** For information about any parameter, click on **Help**.	
7. Click on **OK**.	You are asked whether you want to edit the OSI interface details (parameters).
8. If you answer **No**, click on **Done** and skip the rest of the steps in this table.	OSI appears next to the tunnel name in the GRE Create Tunnels List window, and then you return to the Configuration Manager window.
9. If you answer **Yes**, you can change any of the following parameters: • **Enable** • **Routing Level** • **L1 Default Metric** • **L2 Default Metric** • **L1 Designated Router Priority** • **L2 Designated Router Priority** • **IIH Hello Timer** • **ISH Hello Timer** • **ESH Configuration Timer** • **Circuit Password** • **IIH Hold Time Multiplier** • **ISH Hold Time Multiplier** • **Redirect Enable/Disable** For information about any parameter, click on **Help** or consult the *Configuring OSI Services* guide.	The Edit OSI Interface window opens.
10. Click on **OK**.	OSI appears next to the tunnel name in the GRE Create Tunnels List window.
11. Click on **Done**.	You return to the Configuration Manager window.

Configuring the Remote Tunnel End Point

A *remote tunnel end point* can be any IP interface configured on a Nortel Networks router or another router that complies with RFCs 1701 and 1702. To maximize the robustness of the tunnel, use a circuitless IP address as a tunnel's physical end point whenever possible. For instructions on configuring a circuitless IP interface, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

When you configure a remote tunnel end point, you assign it a name and specify the IP address of the *remote physical interface*. The physical interface is the physical router interface at the remote end of the tunnel. This address is visible to the network cloud that the tunnel passes through.

The *remote logical interface*, required for an IP or an IPX interface, is not visible to the network cloud.

For a remote tunnel end point of this protocol type	You must configure a remote...	
	physical interface	logical interface
IP	✔	✔
IPX	✔	✔
OSI	✔	

For a GRE tunnel configured with an IP, IPX, or OSI protocol, you can configure one or more remote tunnel end points. For more information, see "Number of Tunnels Configurable per Router" on page 1-9.

Using the BCC

To configure a remote tunnel end point using the BCC, complete the following steps.

Step 1. Configuring a Remote Physical Interface

To configure a remote tunnel end point, navigate to the GRE tunnel interface prompt (for example, **box; tunnels; gre/boston**) and enter:

remote-endpoint *<name>* **address** *<address>*

name is the unique name for the remote end of the tunnel.

address is the valid IP address of the router interface at the remote end of the GRE tunnel entered in dotted-decimal notation.

For example, the following command sequence configures the remote end point *austin* with the physical interface 197.1.2.4 and verifies the entry:

```
gre/boston# remote-endpoint austin address 197.1.2.4
remote-endpoint/austin# info
    address 197.1.2.4
    logical-ip-address 0.0.0.1
    logical-ipx-address 000000000001
    name austin
    state enabled
```

Note: When you configure a remote physical end point, the BCC automatically inserts a default address value for the remote logical interfaces. For IP, the default address is 0.0.0.1; for IPX, it is 000000000001. These addresses are not valid. Until you configure valid logical addresses, the tunnel will not come up.

Step 2. Configuring a Remote Logical Interface

Using the BCC, you can configure a logical interface for a remote end point.

Configuring a Remote Logical IP Interface

To configure a remote logical IP interface, navigate to the remote GRE tunnel interface prompt (for example, **box; tunnels; gre/boston; remote-endpoint/austin**) and enter:

logical-ip-address *<address>*

address is a valid IP address expressed in dotted-decimal notation.

For example, the following command sequence configures the remote logical IP interface 9.9.9.2 for the remote tunnel end point *austin* and verifies the change:

```
remote-endpoint/austin# logical-ip-address 9.9.9.2
remote-endpoint/austin# info
name austin
  address 197.1.2.4
  logical-ip-address 9.9.9.2
  logical-ipx-address 000000000001
  state enabled
```

Configuring a Remote Logical IPX Interface

To configure a remote logical IPX interface, navigate to the remote GRE tunnel interface prompt (for example, **box; tunnels; gre/boston; remote-endpoint/austin**) and enter:

logical-ipx-address *<address>*

address is a valid IPX address up to 12 characters in length in hexadecimal notation.

For example, the following command sequence configures the remote logical IPX interface 00112255 for the remote tunnel end point *austin* and verifies the change:

```
remote-endpoint/austin# logical-ipx-address 00112255
remote-endpoint/austin# info
name austin
  address 197.1.2.4
  logical-ip-address 9.9.9.2
  logical-ipx-address 000000112255
  state enabled
```

Using Site Manager

Configuring a Remote End Point for IP or IPX

To configure a remote tunnel end point for either an IP or IPX protocol, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Choose a tunnel from the list, and then click on **Remote Conn**.	The GRE Remote Connections List window opens.
5. Click on **Add**.	The Create GRE Remote Connection window opens.
6. Set the following parameters: • **Connection Name** • **Remote Physical IP Address** • **Remote Logical IP Address** • **Remote Logical IPX Address (hex)** Click on **Help** or see the parameter descriptions beginning on page A-5.	Depending on which protocols you added to the tunnel (IP, IPX, or both), Site Manager allows you to configure the Remote Logical IP Address or the Remote Logical IPX Address (hex) parameter, or both.
7. Click on **OK**.	You return to the GRE Remote Connections List window.
8. Click on **Done**.	You return to the GRE Create Tunnels List window.
9. Click on **Done**.	You return to the Configuration Manager window.

Configuring a Remote End Point for OSI

To configure a remote tunnel end point for the OSI protocol, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Choose a tunnel from the list, and then click on **Remote Conn**.	The GRE Remote Connections List window opens.
5. Click on **Add**.	The Create GRE Remote Connection window opens.
6. Set the following parameters: • **Connection Name** • **Remote Physical IP Address** Click on **Help** or see the parameter descriptions beginning on page A-5.	
7. Click on **OK**.	The connection name appears in the GRE Remote Connections List window.
8. Click on **Done**.	You return to the GRE Create Tunnels List window.
9. Click on **Done**.	You return to the Configuration Manager window.

Customizing a GRE Tunnel

You can customize a configured GRE tunnel, as described in the following sections:

Topic	Page
Disabling and Reenabling a GRE Tunnel	1-21
Disabling and Reenabling a Protocol on a GRE Tunnel	1-22
Deleting a Protocol from a GRE Tunnel	1-24
Disabling and Reenabling a Remote Tunnel End Point	1-25
Deleting a Remote Tunnel End Point	1-26

Disabling and Reenabling a GRE Tunnel

When you create a GRE tunnel, the tunnel is enabled by default. You can use the BCC or Site Manager to disable or reenable it.

Using the BCC

To disable or reenable a GRE tunnel, navigate to the GRE tunnel interface prompt (for example, **box; tunnels; gre/boston**) and enter:

state *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command sequence disables the tunnel *boston* and verifies the change:

```
gre/boston# state disabled
gre/boston# info
   local-address 197.1.2.3
   name boston
   state disabled
```

Using Site Manager

To disable or reenable a GRE tunnel, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Select a tunnel from the list.	
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-4.	
6. Click on **Apply**.	The selected tunnel is enabled or disabled.
7. Click on **Done**.	You return to the Configuration Manager window.

Disabling and Reenabling a Protocol on a GRE Tunnel

When you configure a protocol interface on a GRE tunnel, the interface is enabled by default. You can use the BCC or Site Manager to disable or reenable it. If you want to add an interface to the tunnel for either the IP or IPX protocol, see "Adding a Protocol to the Local Tunnel End Point" on page 1-12.

Using the BCC

To disable or reenable either IP or the IPX protocol, navigate to the protocol interface prompt (for example, **box; tunnels; gre/boston; ip/9.9.9.1/ 255.255.255.0**) and enter:

state *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command disables the IP protocol interface 9.9.9.1/255.255.255.0:

```
ip/9.9.9.1/255.255.255.0# state disabled
```

Using Site Manager

To disable or reenable an IP, IPX, or OSI interface on a GRE tunnel, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**, **IPX**, or **OSI**.	The IP, IPX, or OSI menu opens.
3. Choose **Interfaces**.	The IP Interface List window, IPX Interfaces window, or the OSI Interface Lists window opens, as appropriate.
4. Select the interface that you want to enable or disable from the list.	Site Manager displays the parameter values for that interface.
5. Set the **Enable** parameter.	
6. Click on **Done**.	You return to the Configuration Manager window.

Deleting a Protocol from a GRE Tunnel

Use the BCC or Site Manager to delete a protocol from a GRE tunnel.

Using the BCC

To delete a protocol from a GRE tunnel, navigate to the protocol interface prompt (for example, **box; tunnels; gre/boston; ip/9.9.9.1/255.255.255.0**) and enter:

delete

For example, the following command deletes the IP protocol interface 9.9.9.1/255.255.255.0 from the tunnel *boston*:

```
ip/9.9.9.1/255.255.255.0# delete
gre/boston#
```

Using Site Manager

To delete a protocol from a GRE tunnel, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Select a tunnel from the list, and then click on **Add/Del Prot**.	The Select Protocols window opens.
5. Deselect the protocol.	
6. Click on **OK**.	You return to the GRE Create Tunnels List window.

Disabling and Reenabling a Remote Tunnel End Point

When you configure a remote tunnel end point, it is enabled by default. You can use the BCC or Site Manager to disable or reenable the remote tunnel end point.

Note: If you want to add another remote tunnel end point for the tunnel, see "Configuring the Remote Tunnel End Point" on page 1-16.

Using the BCC

To disable or reenable a remote tunnel end point, navigate to the remote GRE tunnel interface prompt (for example, **box; tunnels; gre/boston; remote-endpoint/austin**) and enter:

state *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command sequence disables the remote tunnel end point *austin* and verifies the change:

```
remote-endpoint/austin# state disabled
remote-endpoint/austin# info
name austin
  address 197.1.2.4
  logical-ip-address 9.9.9.2
  logical-ipx-address 00112255
  state disabled
```

Using Site Manager

To disable or reenable a remote tunnel end point, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Click on **Remote Conn**.	The GRE Remote Connections List window opens.
5. Select the remote tunnel end point that you want to disable or reenable from the list.	
6. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-4.	
7. Click on **Apply.**	The selected tunnel end point is enabled or disabled.

Deleting a Remote Tunnel End Point

Use the BCC or Site Manager to delete a remote tunnel end point from a GRE tunnel.

Using the BCC

To delete a remote tunnel end point, navigate to the remote GRE tunnel interface prompt (for example, **box; tunnels; gre/boston; remote-endpoint/austin**) and enter:

delete

For example, the following command deletes the remote tunnel end point *austin*:

```
remote-endpoint/austin# delete
gre/boston#
```

Using Site Manager

To delete a remote tunnel end point, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Click on **Remote Conn**.	The GRE Remote Connections List window opens.
5. Select the remote tunnel end point that you want to delete, and then click on **Delete**.	A confirmation window opens.
6. Click on **OK**.	The remote tunnel end point is deleted.

Deleting a GRE Tunnel

Use the BCC or Site Manager to delete a GRE tunnel from the router.

Using the BCC

To delete a GRE tunnel, navigate to the GRE tunnel interface prompt (for example, **box; tunnels; gre/boston**) and enter:

delete

For example, the following command deletes the tunnel *boston*:

```
gre/boston# delete
tunnels#
```

Using Site Manager

To delete a GRE tunnel, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Select the tunnel that you want to delete from the list, and then click on **Del Tunnel**.	A confirmation window opens.
5. Click on **OK**.	You return to the GRE Create Tunnels List window.

Chapter 2
Configuring Network Address Translation

This chapter describes network address translation (NAT) and provides instructions for configuring NAT on a router.

Topic	Page
NAT Concepts	2-2
Examining How Different Types of NAT Work	2-13
NAT Implementation Guidelines	2-32
Starting NAT Services and Configuring Translations	2-40
Customizing NAT Global Parameters	2-65
Customizing a NAT Interface	2-74
Configuring NAT Static Address Translation	2-80
Configuring NAT Dynamic Address Translation	2-95
Configuring NAT N-to-1 Translation	2-113

NAT Concepts

Network Address Translation is a method by which IP addresses are mapped from one address realm to another, providing transparent routing to hosts (per RFC 2663). The NAT service implementation for BayRS allows network administrators to configure a Nortel Networks router to be able to translate the source, destination, or both the source and destination IP addresses of packets, for the purpose of forwarding traffic between different networks with otherwise incompatible addresses. For Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) traffic, NAT can also translate port numbers, allowing multiple hosts to share a single address.

To understand how NAT works, think of the router configured with NAT (hereafter referred to as "the NAT router") as situated between two or more domains. In the BayRS implementation of NAT, a *domain* is a network of devices with uniquely assigned IP addresses, such that datagrams can be routed among them. The NAT router borders the network domains where the IP addresses will be translated from or to.

The public Internet can be considered an example of such a domain because any device that connects to it must have a registered, unique address. Another example of a domain would be an enterprise using a nonregistered block of addresses, where care has been taken to avoid duplication of addresses within the enterprise network. Because the enterprise uses nonregistered addresses, it would require a NAT router to connect to the Internet.

You can configure the NAT router for address translations of IP traffic to occur between two or more domains and for translations to be either unidirectional or bidirectional. Both unidirectional and bidirectional NAT can be configured using static and dynamic translation modes.

For more information, see the following topics:

Topic	Page
Unidirectional NAT	2-3
Bidirectional (Multidomain) NAT	2-7
Translation Modes	2-10

Unidirectional NAT

For *unidirectional NAT*, the translation is done for addresses within the source domain to route traffic to an address in a destination domain. When you are configuring NAT, this source domain is given the special name of “private” and the destination domain is given the special name “public.” The translation session must be initiated from a device in the private domain.

The domain known to NAT services as “private” can include network addresses that are unregistered or not globally unique. Such addresses are considered *private addresses.* They are never advertised outside of their network domain. For example, addresses 10.0.0.0 through 10.255.255.255 make up a range that is reserved for use in private networks; it is not valid on the public Internet.

By contrast, the domain known to NAT services as “public” contains standard registered IP addresses that are globally unique. These addresses are *public addresses.* Public addresses are advertised both within and outside of the network domain known as “public.”

Advantages

Unidirectional NAT offers a solution to two problems facing enterprises accessing the Internet:

- The diminishing number of available IP addresses for Internet hosts
- Private networks with unregistered addresses that cannot access the Internet

Using NAT, you can create a pool of registered IP network addresses that the router can dynamically map to the unregistered host addresses in your local network. If an enterprise does not have enough globally unique IP addresses for each host on its network, NAT can allow for the sharing of a limited number of registered IP addresses by allocating them for use only as needed.

Requirements

In addition to configuring NAT on the router, unidirectional NAT (including unidirectional types SDPT and N-to-1) requires that you:

- Configure IP on each router interface to be configured with NAT.
- Configure Routing Information Protocol (RIP), RIP2, or static routes on the NAT router interfaces. You must also configure RIP or static routes on each device in the domain "private" that passes traffic into the NAT router for address translation and on each device in the domain "public" that passes traffic with translated addresses out of the NAT router.

For More Information About Unidirectional NAT

For an example of how unidirectional NAT works, see:

- "Static Unidirectional Address Translation" on page 2-14
- "Dynamic Unidirectional Address Translation" on page 2-15

Before you configure unidirectional NAT for the first time, consult the section "NAT Implementation Guidelines" on page 2-32.

To configure unidirectional NAT, see:

- "Configuring Unidirectional NAT (Dynamic)" on page 2-40
- "Adding a Static Unidirectional Address Mapping" on page 2-81

To view available NAT statistics during or after you configure bidirectional NAT, consult the following:

For this information	See
BCC **show nat** and **show ip** commands	*Reference for BCC IP show Commands*
NAT log messages	"Logging NAT Messages" on page 2-69

Representing Multiple Hosts with a Single Address: SDPT and N-to-1

For TCP and UDP traffic, you can configure network address translation of many private addresses to a single public address. Some applications that use TCP are File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP), and Telnet. Trivial File Transfer Protocol (TFTP) is an application that uses the UDP protocol.

For TCP and UDP traffic, there are two types of possible network address translation types. Table 2-1 compares these unidirectional types, static destination and port translation (SDPT) and N-to-1.

Table 2-1. Comparing NAT Types SDPT and N-to-1

	SDPT (One to Many)	**N-to-1 (Many to One)**
Definition	SDPT allows you to configure a single public IP address to be translated to many private addresses.	N-to-1 allows you to configure a range of addresses in a private network to be translated into a single, public IP address.
Packet type	Valid for TCP or UDP packet forwarding only	Valid for TCP or UDP packet forwarding only
Translation direction	Supported for unidirectional NAT only; the supported translation direction is *public to private**	Supported for unidirectional NAT only; translation direction is *private to public*
Static vs. dynamic configuration: address and port	The user must statically configure both address and port translation. SDPT uses the translated port to distinguish between application types such as FTP and TFTP. The port is also used to determine the destination host on the private side of the NAT router.	The user must statically configure address translation. Port numbers are assigned dynamically when the NAT router maps a private address to the public address.
Aging	SDPT mappings remain in the NAT translation table until you disable or delete them.	N-to-1 mappings are removed from the NAT translation table after a specified timeout period, unless the mapping aging (timeout) parameter is disabled.

* Although SDPT can be initiated from the private as well the public side, Nortel Networks recommends that you implement this type of configuration with a simple static translation; it is not common that a network administrator would need to translate a port from a host in a private domain to a destination in a public domain.

The major difference between SDPT and N-to-1 translation is that N-to-1 applies only for sessions initiated from the private domain, while SDPT allows sessions to be initiated from the public domain. By configuring NAT N-to-1, an enterprise using unregistered addressing on its internal network can use the NAT router to translate those unregistered addresses into a single registered IP address, or multiple IP addresses, for the purpose of making connections to the Internet.

SDPT typically provides support for a single application, such as HTTP or FTP, because with NAT SDPT each private host is uniquely identified by a statically defined port.

For More Information on SDPT and N-to-1

For an example of how the translation types SDPT and N-to-1 work, see:

- "Static Destination and Port Translation (SDPT)" on page 2-20
- "Network Address Port Translation (N-to-1)" on page 2-23

Before you configure unidirectional SDPT or N-to-1 for the first time, consult the section "NAT Implementation Guidelines" on page 2-32.

To configure these translation types, see:

- "Adding an SDPT Address and Port Mapping" on page 2-89
- "Configuring NAT N-to-1 Translation" on page 2-113

To view available NAT statistics during or after you configure SDPT or N-to-1, consult the following:

For this information	See
BCC **show nat** and **show ip** commands	*Reference for BCC IP show Commands*
NAT log messages	"Logging NAT Messages" on page 2-69

Bidirectional (Multidomain) NAT

Bidirectional multidomain NAT is a unique feature of BayRS that enables:

- A single NAT router to support address translation among two or more domains
- Sessions to be initiated from any one domain to any other domain
- Hosts in domains with overlapping address space to communicate with each other, similar to what is known as "twice NAT" (for more information, see RFC 2663).

Address translation between the source domain and the destination domain of the NAT router can be initiated from any domain connected to the NAT router. In bidirectional multidomain NAT, both the source address and destination address are translated by the NAT router. For ease of reference in this guide, the term bidirectional NAT is used interchangeably with, and has the same meaning as, bidirectional multidomain NAT.

Advantages

Bidirectional NAT allows you to translate IP addresses on a NAT router connected to two or more domains. As a network administrator, you might use a bidirectional NAT configuration to allow:

- Users to initiate traffic from either side of a router configured with NAT
- Hosts in two domains with overlapping address space (with duplicate addresses) to communicate with each other
- A NAT router to represent an address in one domain as a different address in another domain

Requirements

In addition to configuring NAT on the router, bidirectional NAT requires that you:

- Configure IP on each router interface to be configured with NAT
- Configure RIP2 on the NAT router interfaces and on each router that will be exchanging routing updates in the domains of your bidirectional NAT configuration. Otherwise, you must configure static routes or a combination of RIP2 and static routes.

- Install Domain Name System (DNS) server on a machine with a public interface to the NAT router. (DNS server software is available from third-party suppliers.)
- Configure BayRS DNS proxy on each interface of a NAT router to be used for *dynamic* bidirectional translation. Although you can also configure DNS proxy for a *static* bidirectional network address translation, DNS proxy is not required.
- Configure BayRS DNS client on each device in the domains of your bidirectional NAT configuration that will be initiating translations on the NAT router.

The domain names that you specify in your bidirectional NAT configuration can be any name that is in accordance with RFC 1035. You cannot assign the special names of "public" and "private" because these are reserved for use in configuring unidirectional NAT.

How DNS Server, DNS Client, and DNS Proxy Work with Bidirectional NAT

BayRS *DNS proxy server* enables a Nortel Networks router to act as a DNS server. Each instance of the DNS proxy server on the router contains a list of servers to contact on behalf of the client.

Clients on a local area network (LAN) typically use DNS servers to obtain the IP address of a host based on the host's domain name. You must configure BayRS DNS client software on each device that can initiate translations through the NAT router in your bidirectional NAT configuration.

Each DNS request from any address domain used by NAT must come through the NAT router. The DNS proxy server asks NAT for an address translation and replaces the address information in the DNS packet with the translated addresses. NAT puts these addresses in its translation table at the same time. When the client host makes an IP request for the service it asked for in DNS, the client finds the correct path to the destination because NAT already has the destination IP addresses in its translation tables.

The DNS proxy server accepts DNS name service requests from hosts on either side of the router configured for bidirectional NAT and forwards these requests to a preconfigured external DNS server. When the DNS replies come back, the DNS proxy server queries NAT services and determines whether the DNS returned addresses need to be translated. NAT then supplies translated addresses to the DNS proxy server, as appropriate.

For more information about DNS, see *Configuring IP Utilities*.

For More Information on Bidirectional NAT

For an example of how bidirectional NAT works, see:

- "Static Bidirectional Address Translation" on page 2-26
- "Dynamic Bidirectional Address Translation with Two Domains" on page 2-28
- "Dynamic Bidirectional Address Translation with Three Domains" on page 2-29

Before you configure unidirectional NAT for the first time, consult the section "NAT Implementation Guidelines" on page 2-32.

To configure bidirectional NAT, see:

- "Configuring Bidirectional NAT (Dynamic)" on page 2-50
- "Adding a Static Bidirectional Address Mapping" on page 2-84

To view available NAT statistics during or after you configure bidirectional NAT, consult the following:

For this information	**See**
BCC **show nat** and **show ip** commands	*Reference for BCC IP show Commands*
NAT log messages	"Logging NAT Messages" on page 2-69

Translation Modes

You can configure your router so that network address translation occurs in one or more of the following translation modes:

- *Static translations* are the result of mappings of one address to another as specified by the user. A static translation remains active until it is disabled or deleted.
- *Dynamic translations* are triggered by host traffic whenever the NAT router receives a packet whose source address falls within a specified filter range. You configure possible address translations in advance of the translation request. A dynamic address translation remains active until the specified timeout.

Static Translation Mode

NAT static mode allows you to statically configure a translation address for a private or unregistered address. The translated address will then be used to represent the private host for any packets sent outside its private domain. Static translations are for addresses from two domains.

Static address translation is possible on any NAT interface. You can statically configure addresses for unidirectional NAT (including SDPT and N-to-1) and bidirectional NAT. When configuring static NAT translations, two mapping entries cannot share either the same original IP address or the same translated IP address.

Configuring NAT in static mode is especially useful for address translation among a few hosts. Static address mappings can be used to preserve a translation entry or to create a connection from a host on the public network to a host on the private network, or vice versa.

For an example of how a static unidirectional translation works, see "Unidirectional NAT" on page 2-14. For instructions on how to configure static translation, see "Configuring NAT Static Address Translation" on page 2-80.

A static address translation mapping does not time out as dynamic translations do, but remains active as long as the static mapping has not been disabled or deleted. For instructions on how to disable or delete a static mapping, see:

- "Disabling and Reenabling a Static Address Mapping" on page 2-92
- "Deleting a Static Address Mapping" on page 2-93

Dynamic Translation Mode

NAT dynamic translation mode allows you to configure a temporary mapping of private domain addresses to an address pool of public addresses in the same domain or in another domain. For dynamic NAT to function, you must configure a source address filter and a translation pool.

- A *source address filter* is a range of addresses that you specify as requiring dynamic translation by the NAT router. The source addresses are replaced by NAT with ones from its associated translation pool. The source address filter is similar to the term *local address range* used in NAT for BayRS versions before Version 14.20.

  For unidirectional NAT, the translation pool addresses associated with the source address filter are located in the destination, outbound domain. For bidirectional NAT, you can specify whether to use a translation pool defined for the source, inbound domain or the destination, outbound domain.

- A *translation pool* is a range of IP addresses that you specify for the NAT router to use when dynamically translating the source address, for unidirectional NAT, or the source and destination addresses, for bidirectional NAT for IP packets requiring address translation. The translation pool is similar to the term *global address range* used in NAT for BayRS versions before Version 14.20.

Address range considerations for dynamic translation mode

Using dynamic NAT, you can configure multiple source address filters and translation pools for use within the same domain, provided the address ranges do not overlap. That is, the address ranges specified for one source address filter must not match another source address filter in the same domain, and the same is true of addresses between translation pools within the same domain. Overlapping address ranges are allowed between dynamic and static NAT configurations. For more information on multiple source address filters within the same domain, see "Multiple Source Address Filters -- Order of Precedence for NAT Types" on page 2-35.

When configuring source address filters or translation pools for different domains, you can use the same address range in one source address filter or translation pool as you use for another source address filter or translation pool in a different domain. For example, you can configure the address range 22.1.1.1/8 for a translation pool in both domain1.net and domain2.net.

Comparing unidirectional and bidirectional dynamic NAT

You can configure unidirectional or bidirectional NAT for dynamic translation.

For dynamic unidirectional NAT:

- When a router configured with NAT detects an *outbound* packet from an address within a configured source address filter, NAT uses the translation pool from which to map a public, registered address from a domain named "public." NAT replaces the packet's original address with the public address, and sends the outbound packet to its destination address in the domain named "public."
- When a router configured with NAT detects an *inbound* packet for a destination address that falls within the configured translation pool, it replaces the packet's public destination address with the original address and sends the packet to its destination on the domain named "private."

For dynamic bidirectional NAT, when the NAT router detects an address that matches a source address filter, the source and destination addresses are translated into the next available address from a translation pool. You specify whether this translation pool is in the same domain or in a different domain than the source address filter.

For more information on dynamic translation mode

For examples of how dynamic network address translation works, see:

- "Dynamic Unidirectional Address Translation" on page 2-15
- "Dynamic Bidirectional Address Translation with Two Domains" on page 2-28
- "Dynamic Bidirectional Address Translation with Three Domains" on page 2-29

For instructions on how to create and enable dynamic address translation, including source address filters and translation pools, see "Configuring NAT Dynamic Address Translation" on page 2-95.

Dynamic NAT translations are active until the specified mapping timeout value is reached. The translation remains in a translation table for as long as it is active. An idle entry is removed after a specified timeout period. If the timeout parameter is disabled, the mapping is not removed.

For instructions on how to configure mapping aging, see:

- "Enabling and Disabling the Dynamic Mapping Aging Timer" on page 2-71
- "Configuring the Dynamic Mapping Timeout Value" on page 2-72

Examining How Different Types of NAT Work

The following sample translations illustrate the different ways in which you can configure NAT for IP address and port translations:

For this type of unidirectional NAT	Go to page
Static Unidirectional Address Translation	2-14
Dynamic Unidirectional Address Translation	2-15
Static Destination and Port Translation (SDPT)	2-20
Network Address Port Translation (N-to-1)	2-23

For this type of bidirectional NAT	Go to page
Static Bidirectional Address Translation	2-26
Dynamic Bidirectional Address Translation with Two Domains	2-28
Dynamic Bidirectional Address Translation with Three Domains	2-29

To help illustrate how NAT works, the figures in this section contain address information such as host, interface, source address filter, translation pool, and translation table addresses. To view similar information about your actual NAT configuration, use the BCC **show ip** or **show nat** commands. There are also **show nat** scripts available through the Technician Interface. For more information, refer to "Checking Address Translations" on page B-10.

Unidirectional NAT

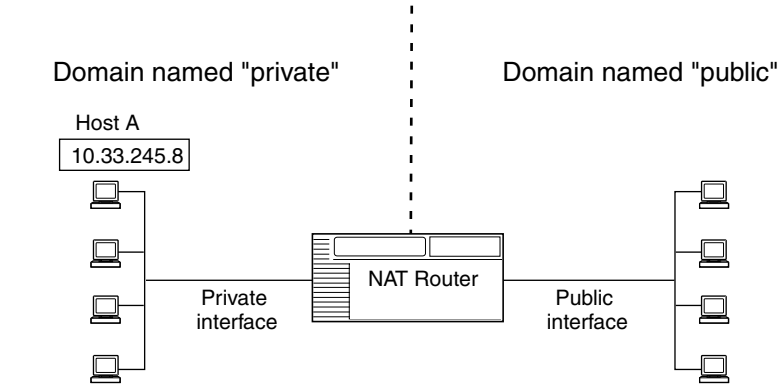
You can configure the following types of unidirectional NAT: static unidirectional NAT, dynamic unidirectional NAT, SDPT, and N-to1.

Static Unidirectional Address Translation

For a static, unidirectional network address translation, you must configure:

- A router with IP and NAT
- A private NAT router interface that belongs to the domain “private”
- A public NAT router interface that belongs to the domain “public”
- A static mapping pair of one host IP address (typically unregistered) in the domain “private” to be translated into a registered IP address of a host in the domain “public.” For example, you could statically map the private address 10.33.245.8 to the registered address 192.142.59.32 as shown in Figure 2-1.

Then, based on this static mapping pair, the NAT router can use the registered, public IP address 192.142.59.32 for the host 10.33.245.8 when the host needs to make a connection to the Internet, say for a destination address of 66.123.5.74.



Static mapping on NAT router

Source/inbound domain	Original/private address	Translated/public address	Destination/outbound domain
private	10.33.245.8	192.142.59.32	public

IP0121A

Figure 2-1. Static Unidirectional NAT Configuration

Dynamic Unidirectional Address Translation

NAT routers translate host addresses from inside private networks into registered addresses that can be used in the public network. On its return trip, a packet using a NAT-assigned registered address destined for the internal network is translated back into its original private address. NAT maintains a table of current translations. Translations remain in the table until they become inactive and time out, freeing up the registered public address for use by other hosts.

In the example that follows, company A uses NAT to obtain public Internet access for its hosts. Hosts on company A's network need access to resources in company B's network. Company B is located in a different network on the Internet. Its addresses are registered. NAT is configured on the router bordering company A's network and the public network. NAT enables communication between the networks of company A and company B without requiring either company to restructure its existing network.

The network administrator at company A configures NAT to detect the following ranges of unregistered private addresses:

- 10.0.0.0 through 10.255.255.255
- 15.0.0.0 through 15.255.255.255
- 50.1.1.0 through 50.1.1.255

The network administrator also configures the following ranges of registered public addresses:

- 192.55.10.0 through 192.55.10.255
- 192.20.10.0 through 192.20.10.255

In Figure 2-2, a packet from company A's network with unregistered source address 10.0.0.15 is sent to a destination address in company B's network. The destination is a publicly recognized registered address, 192.100.20.2. The packet follows normal IP routing to the NAT border router at the egress point in company A, the NAT router in Chicago.

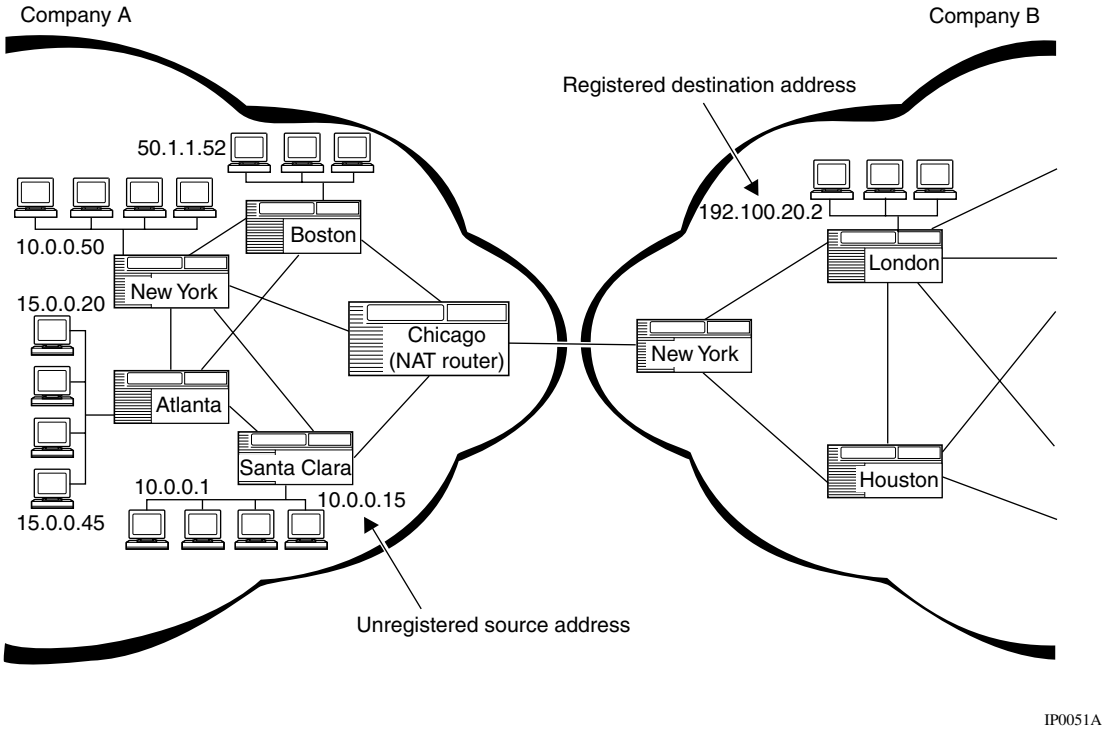


Figure 2-2. Network Address Translation Example

When the router's NAT interface receives a packet, the NAT router extracts the source address, first checking whether the packet's source address falls within a configured source address filter. If it does, NAT compares the source address against existing address translation entries in its translation table. In Figure 2-3, the NAT router detects a packet on a NAT interface that contains the address 10.0.0.15.

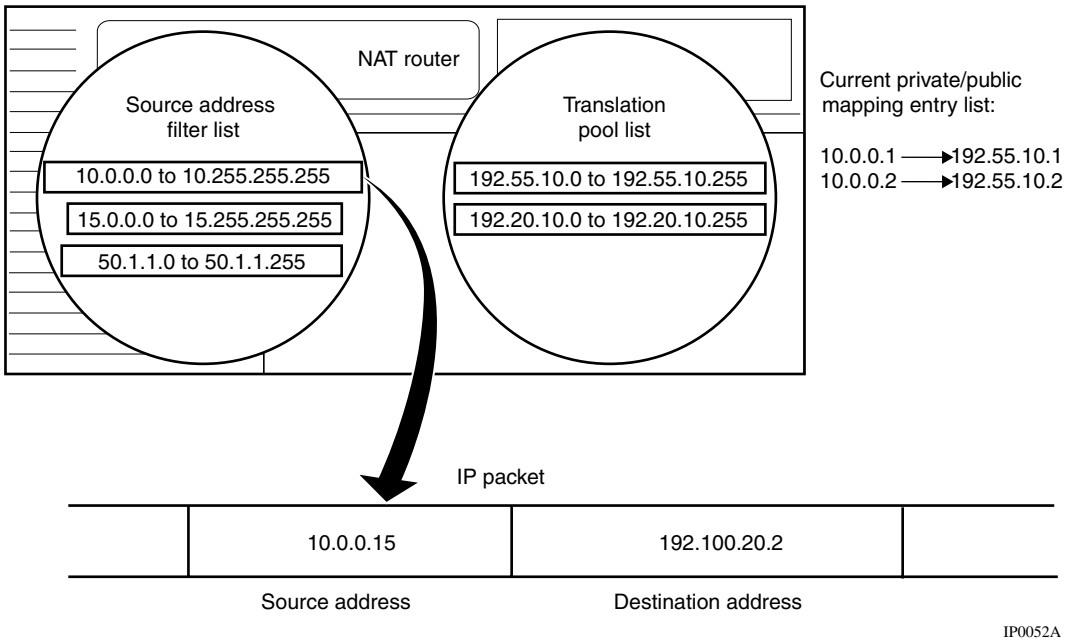


Figure 2-3. NAT Detects the Source Address

If the host's source address does not appear in the translation table and is within a configured source address filter, the NAT router does the following:

1. Creates a new entry for the host
2. Dynamically assigns the next available, lowest registered IP address from a translation pool
3. Changes the source address of the packet to the registered address

In Figure 2-4, the NAT router dynamically translates the source address, 10.0.0.15, to one of the available public addresses (in this case, 192.55.10.3) and creates a new entry in the private/public translation entry list.

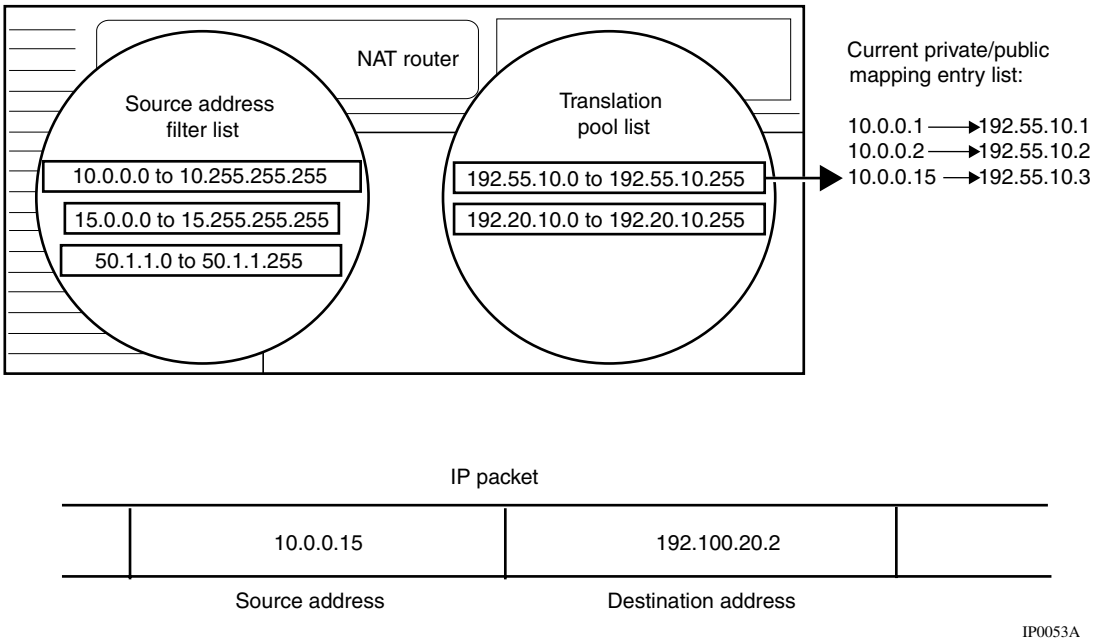


Figure 2-4. NAT Updates the Private/Public Translation Entry List

In Figure 2-5, the NAT router then replaces the private source address (10.0.0.15) with the translated public address (192.55.10.3) and sends the packet on its way to its destination in company B's network.

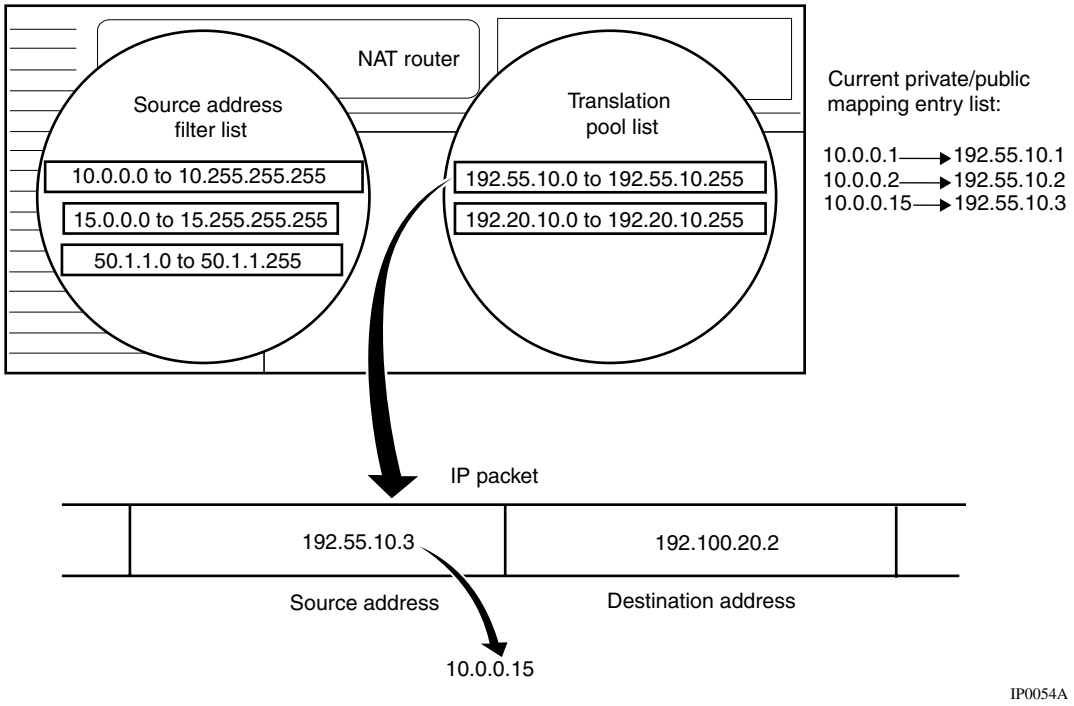


Figure 2-5. NAT Replaces the Private Address with a Registered Source Address

The destination host uses the incoming packet's source address to create a destination address to send a packet back to the sending host. When the packet arrives at company A's NAT router:

1. The NAT router checks the packet's destination address. If it is a public address from a configured translation pool, NAT compares the destination address to entries in its translation table.
2. If the NAT router finds the public IP address in the translation table, it replaces the destination address with the original private address.

After a specified timeout period during which there have been no translated packets for a particular address translation, company A's NAT router removes the mapping, freeing the public address for use by another inside host.

Static Destination and Port Translation (SDPT)

You can use static destination port translation to map a single public address to many private addresses (one-to-many). SDPT is a unidirectional translation type that translates from the domain named "public" to the domain named "private." NAT SDPT requires that you statically configure an original port and a translated port. SDPT uses the translated port to distinguish between application types such as FTP and TFTP.

Note: SDPT translation is valid only for TCP or UDP packets. All non-TCP or non-UDP packets with addresses that fall within the configured local address range are dropped.

SDPT is intended primarily for situations where a server in the private domain supports a particular application for users in the public domain. In this example, the device at host A in a public domain network would like to initiate an HTTP connection with an HTTP server in a private domain network. To initiate this connection from a public network to a private network, you can configure a router with NAT, such as the one shown in the center of Figure 2-6.

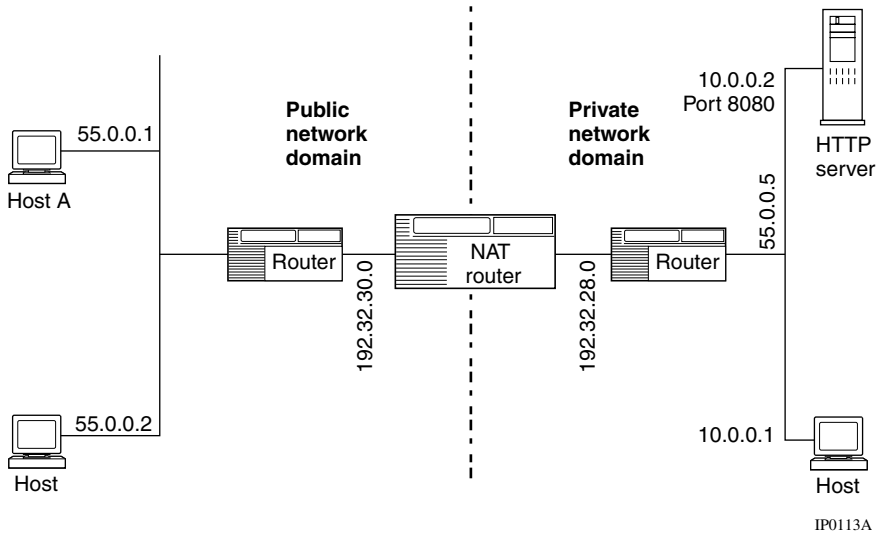


Figure 2-6. Sample Configuration for NAT SDPT

The HTTP server actually has a local IP address of 10.0.0.1 and a port number of 8080. However, in the translation table on the central NAT router, the HTTP server is represented to the public network with a virtual public address of 192.32.29.17 and a virtual port number of 80. So, Host A sends a TCP packet using destination address 192.32.29.17 and destination port 80.

When the packet arrives at the global IP interface of the NAT router, NAT picks up the packet and recognizes that the destination address is an SDPT "public address." It looks in the NAT translation table to find the translation information. NAT translates the destination address and destination port to the address and port of the HTTP server (10.0.0.1 address and 8080 port) in the private network. Then the packet is forwarded to the HTTP server.

The HTTP server sends a reply to host A with source address 10.0.0.1, source port 8080, and the destination address of host A (55.0.0.2). This packet is received by the NAT private domain interface of the NAT router. NAT recognizes the source address as an SDPT "private address" and translates the source address to the virtual address 192.32.29.17 and the source port to the virtual port 80.

It might seem as if this HTTP server has two identities: The server has its actual identity on the private side (10.0.0.1 address and 8080 port) and the other is its virtual identity (192.32.29.17 address and 80 port) on the public side. To initiate a connection with the HTTP server, a host in the private domain uses the server's private (actual) identity and a host in the public domain uses the server's public (virtual) identity.

The host at 10.0.0.1 (seen in the public domain as having the address 192.32.29.17) could also be used as a TFTP server. For example, assume the following configuration shown in Table 2-2 for the NAT router in Figure 2-6.

Table 2-2. Sample Configuration for a Router Configured with NAT

NAT Config.	translation-type	private-address	public-address	private-port	public-port	protocol
1	SDPT	55.0.0.1	192.32.29.17	8080	80	TCP (HTTP)
2	SDPT	55.0.0.1	192.32.29.17	69	69	UDP (TFTP)
3	SDPT	55.0.0.2	192.32.29.17	23	2023	TCP (Telnet)
4	Static	55.0.0.1	192.32.29.17	0	0	0 (Any)
5	N-to-1	33.0.0.0/8	192.32.29.17	Any	Dynamically assigned	TCP/UDP

The first row represents the configuration for the server to handle HTTP traffic; the second row represents the configuration used for this server to act as a TFTP server. *Private-port* is the port the server listens to in the private side of the network; *public-port* is the port to which hosts in the public domain connect.

To act as a TFTP server, this same server listens for TFTP on private port 69. The server needs to have a public-address identity that the user configures. The public address is 192.32.29.17 and the port is 69. By convention, port number 69 is the reserved port for TFTP. Any host in the public domain network that transfers files using TFTP from this server sends UDP packets to IP address 192.32.29.17 and port 69.

To use a different host but the same public address for Telnet services, you could configure the router with the information in the third row of Table 2-2.

When TCP packets with a destination address of 192.32.29.17 arrive in the NAT-configured public interfaces, the NAT router translates the destination port and address to direct the packets to private address 10.0.0.2 and port 23. Note that SDPT translations are exercised first. The static translation (configured in the fourth row of Table 2-2) is used only when an SDPT translation is not found or when the packet is neither TCP or UDP (remembering that SDPT works only with these types of packets).

The N-to-1 translation configuration (configured in the fifth row of Table 2-2) uses the same global address (N-to-1 address) as the first SDPT translation.

Network Address Port Translation (N-to-1)

Using network address port translation (N-to-1), you can map many private addresses to one public address (many-to-one). With N-to-1 translation, you statically configure the address translation and NAT dynamically executes the port translation. The original port is determined by the application running on the host device that is sending packets to the NAT router. N-to-1 is a unidirectional NAT type that translates addresses from the domain named "private" to a single address in the domain named "public."

Note: N-to-1 translation is valid only for TCP or UDP packets. All non-TCP or non-UDP packets with addresses that fall within the configured local address range are dropped.

When NAT receives a packet on the private interface, the following events occur:

1. NAT determines that the private source address falls within the source address filter configured for N-to-1 translation.
2. NAT assigns the packet a public source address based on the statically configured N-to-1 address and dynamically assigns the next available unique port number.
3. NAT transmits the packet on the public interface.

For example, in Figure 2-7 the network administrator has set up a private address range of 10.0.0.0 through 10.255.255.255 in a source address filter and associated this range of private addresses with public IP address 192.1.1.1.

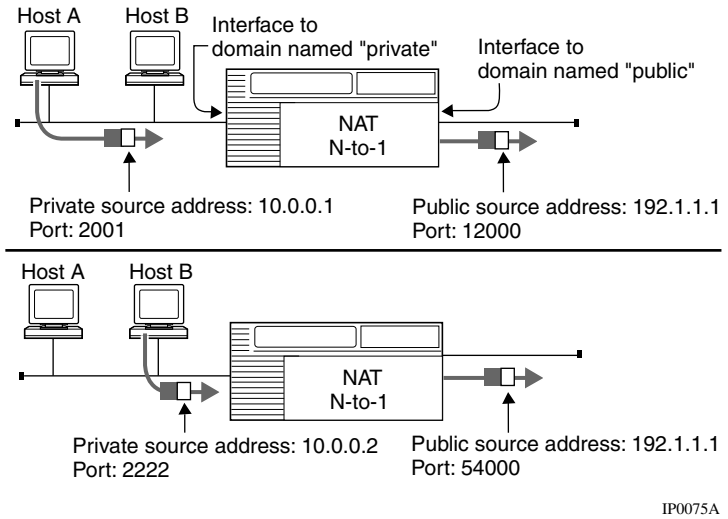


Figure 2-7. N-to-1 Translation (Part 1)

The following events occur:

1. NAT receives a packet from host A on the private interface with a source address of 10.0.0.1 and a port number of 2001.
2. Determining that the private source address falls within the range configured for N-to-1 translation, NAT stores the port number, replaces the private source address with the public address 192.1.1.1, replaces the private port number with the unique port number 12000, and transmits the packet on the public interface.
3. Subsequently, NAT receives a packet from host B on the private interface with private source address 10.0.0.2 and port number 2222. Determining that this private source address falls in the same configured range, NAT replaces the private source address with the public address 192.1.1.1, replaces the private port number with the unique port number 54000, and transmits the packet on the public interface.

When NAT receives a packet from a remote source on the public interface, the following events occur:

1. NAT determines that the destination address on the packet is an N-to-1 address.

2. NAT uses the address and the port number to identify the destination host.
3. NAT replaces the destination IP address and TCP (or UDP) port number with the original private address and port number and transmits it on the private interface.

For example, in Figure 2-8 the following events occur:

1. NAT receives a packet on the public interface with the destination address 192.1.1.1 and port number 12000.
2. Determining that the destination address is an N-to-1 address, NAT uses the address and the port number to locate the destination host, host A. NAT replaces the public destination address and TCP (or UDP) port number with the private address and port number and transmits the packet on the private interface.

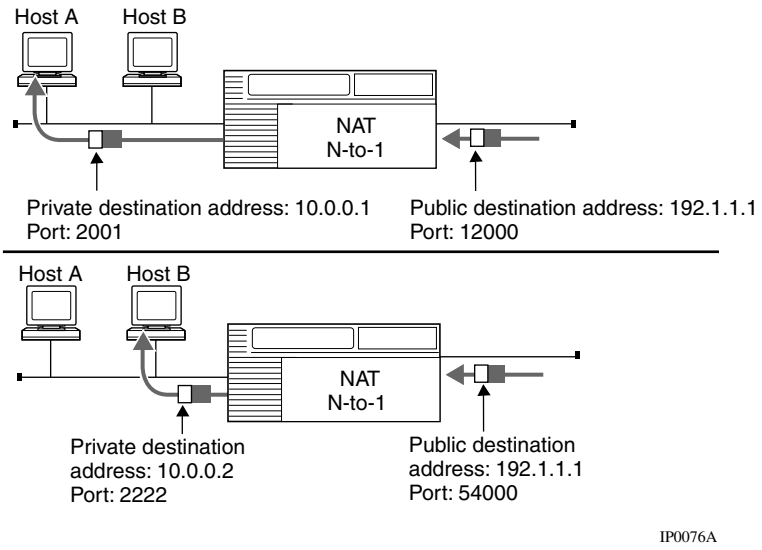


Figure 2-8. N-to-1 Translation (Part 2)

3. Subsequently, NAT receives a packet on the public interface with the destination address 192.1.1.1 and port number 54000. Determining that the destination address is an N-to-1 address, NAT uses the address and the port number to locate the destination host, host B. NAT replaces the public destination address and TCP (or UDP) port number with the private address and port number and transmits the packet on the private interface.

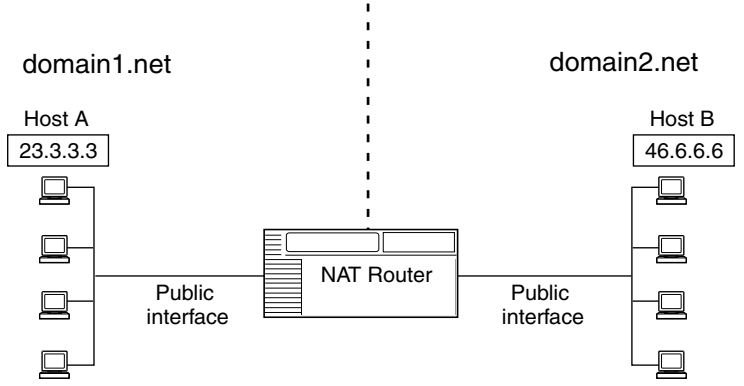
Bidirectional NAT

You can configure bidirectional NAT statically or dynamically, and with two or more domains.

Static Bidirectional Address Translation

Choose static bidirectional NAT when you want to map just a few individual addresses for NAT, with translations being initiated from different domains. Packets sent to the NAT router from statically mapped hosts in either domain will have their source and destination addresses translated by NAT.

For example, Figure 2-9 presents host A in domain 1 and host B in domain 2, with a NAT router between these two domains. You could statically map host A's address 23.3.3.3 in domain 1 to the translation address 89.9.9.9, identifying the domain name to which the NAT router will pass the IP packet.



Static mappings on NAT router

Source/inbound domain	Original/private address	Translated/public address	Destination/outbound domain
domain1.net	23.3.3.3	89.9.9.9	domain2.net
domain2.net	46.6.6.6	57.7.7.7	domain1.net

IP0120A

Figure 2-9. Static Bidirectional NAT Configuration

When host A transmits packets to the NAT router, NAT replaces the source address in the IP packet with the translation address 89.9.9.9. Likewise, if host B in domain 2 transmits packets into the NAT router, the outgoing IP packet would bear the source address 57.7.7.7.

For bidirectional NAT, you must create a minimum of one such static mapping in at least two domains so that host devices in either domain can initiate an address translation by the NAT router. IP packets with translated source addresses can then be passed out of the router to an alternate domain.

The configuration of DNS proxy, required for dynamic bidirectional NAT, is optional for static bidirectional NAT. If you do not configure DNS proxy on the NAT router, you must statically configure one mapping for each domain as described above. However, if you do configure the NAT router as a DNS proxy server, you must statically configure a minimum of two address mappings for each domain, one for the inbound domain and one for the outbound domain. For more information see "Adding a Static Bidirectional Address Mapping" on page 2-84.

Dynamic Bidirectional Address Translation with Two Domains

Figure 2-10 offers an example of bidirectional multidomain NAT with two domains. DNS proxy is configured on the NAT router, a requirement for dynamic bidirectional NAT. In this sample configuration, two private hosts (A and B) with the same address can communicate with each other in either direction using the public interfaces on either side of the NAT router configured with DNS proxy.

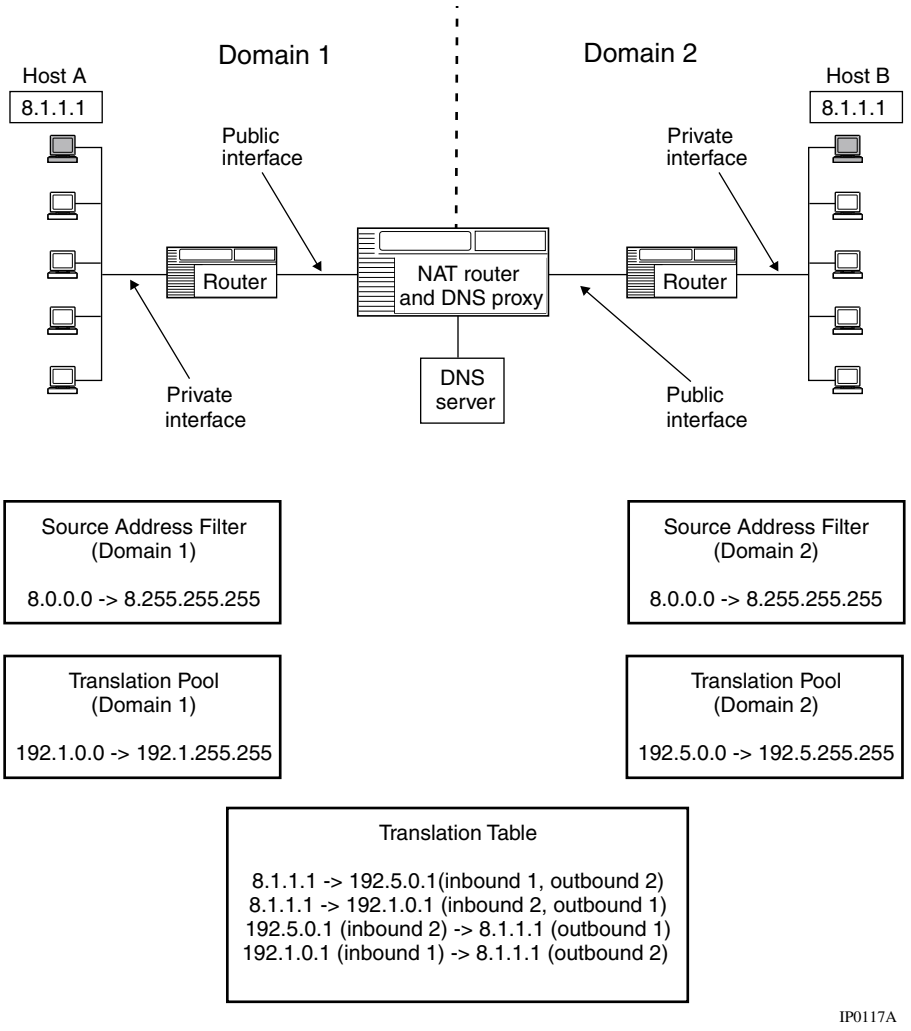


Figure 2-10. Bidirectional NAT with DNS Proxy

A source address filter and translation pool are configured in each domain. Host A in domain 1 generates a request to the DNS server to identify the address of host B located in domain 2. Because the address of host B, located by the DNS server, falls within the range of the source address filter configured for domain 2, the NAT router translates this address and modifies the DNS reply to include the translated address of host B.

Using the translation address in the destination address field of the IP header, host A sends the packet to host B. The NAT router translates the destination address back to its domain 2 representation. At the same time, the NAT router translates the source address (host A's private address) to a translation address to represent host A in domain 2.

For instructions on how to configure a similar dynamic NAT configuration using the BCC, see Appendix B, "Sample Bidirectional NAT Configuration."

Dynamic Bidirectional Address Translation with Three Domains

Figure 2-11 shows an example of NAT in which the NAT router has configured interfaces to three domains. This is a dynamic translation with DNS proxy configured on the NAT router. In this example, a user at host A makes a connection request, such as **ftp hostb.domain3**. Host A at domain 1 sends a DNS request packet to the DNS server in its local domain. The local DNS server forwards the request to the DNS proxy server on the NAT router, asking for the address of host B in domain 3.

The DNS request packet is received by the NAT router DNS proxy. DNS proxy formats a new DNS request packet with the source address equal to the IP address of the interface (192.33.1.1) that the DNS request came in on, and the destination address is set to the address of the DNS server (130.1.1.1) in the target host's domain.

The DNS server in the target host domain (3) receives the DNS request and sends back a DNS response containing the address of host B (44.1.1.1), the target host, to the DNS proxy. The DNS response packet is received by the NAT router DNS proxy. DNS proxy asks for and receives from NAT a translation address (128.1.0.2) for host B at domain 3 (44.1.1.1) contained in the DNS response.

DNS proxy modifies the DNS response message using the translation address (128.1.0.2) it received from NAT. The modified DNS response message is transmitted to the client host, host A (3.1.1.1) in the originating domain (1).

Host A in domain 1 receives the DNS response message and saves the translation IP address (128.1.0.2) of host B in domain 3. Host A in domain 1 starts to send packets to host B in domain 3. The first packet is the FTP open packet. The packets will have a source address of 3.1.1.1 (host A's IP address) and a destination address of 128.1.0.2 (host B's translation address).

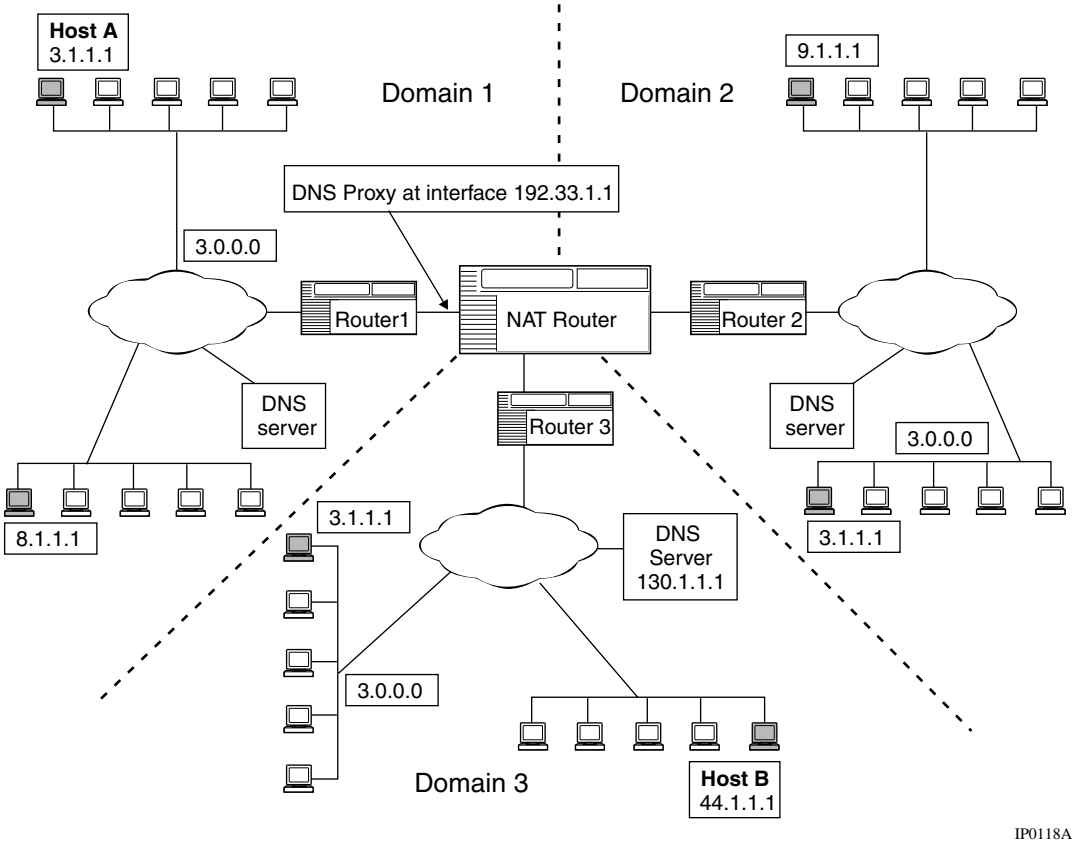


Figure 2-11. Bidirectional NAT with Three Domains

The NAT router receives packets on domain 1's interface from host A destined for host B. NAT replaces the translated destination address (128.1.0.2) with host B's domain specific address (44.1.1.1). NAT replaces host A's domain-specific source address (3.1.1.1) with the domain 3 translation address for host A (128.3.0.1).

Host B receives packets from and sends replies back to host A. The reply packets will have a source address of 44.1.1.1 (host B's IP address) and a destination address of 128.3.0.1 (host A's translation address). NAT receives packets on domain 3's interface. NAT replaces the translated destination address (128.3.0.1) with host A's domain-specific address (3.1.1.1).

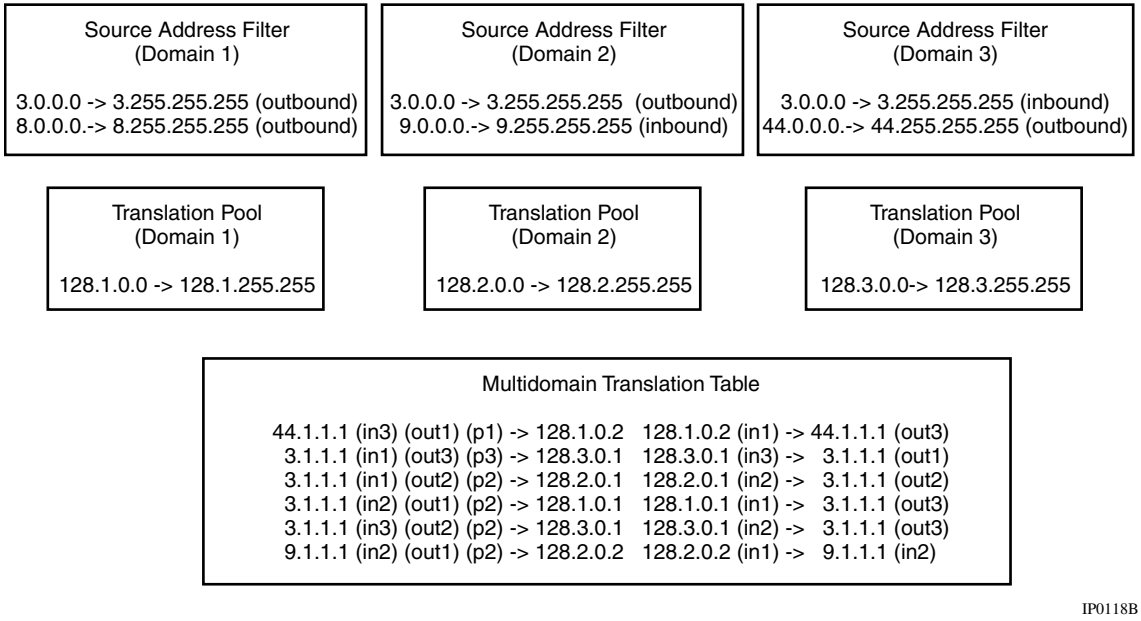


Figure 2-12. Network Address Translations Associated with Figure 2-11

NAT also replaces host B's domain-specific source address (44.1.1.1) with host B's domain 1 translation address (128.1.0.2). Note that host B's domain 1 translation address is defined here as the address for packets originating from host B when they are sent to domain 1. A different translation address may be used for host B when host B sends packets to other domains.

Host A receives packets from host B. The process is repeated until the FTP session is done.

NAT Implementation Guidelines

Before you implement a NAT configuration, you should be aware of the following information.

Topic	Page
NAT General Configuration Considerations	2-32
Protocol Requirements and Compatibilities	2-33
Multiple Source Address Filters -- Order of Precedence for NAT Types	2-35
Internet Control Message Protocol and Message Handling	2-39

NAT General Configuration Considerations

For NAT to function, at a minimum you must configure a NAT interface to a device in each domain. You can configure multiple NAT router interfaces to a single domain to be used in your NAT configuration.

- For unidirectional NAT, you must configure at least one router interface to be in the private domain and one interface to be in the public domain. These interfaces, are known as the *private interface* (has private address) and the *public interface* (has public address), respectively.
- For bidirectional multidomain NAT, you must configure NAT on a router interface to each domain that will be used for network address translation. The interface between the NAT router and each respective domain in a bidirectional configuration must be a public IP address.

You must configure as a NAT interface any network interface that is used to forward packets that have been translated by NAT. Otherwise, packets may be dropped.

The network address translations occurring in one domain must be independent of the translations occurring in the opposite direction. For this reason, each NAT interface must be assigned to only one domain. However, a domain can have more than one NAT interface configured for it.

Note: NAT does not support address translations for addresses that exist within a packet payload, with the exception of DNS requests (bidirectional NAT) and the FTP **port** command (unidirectional NAT).

Protocol Requirements and Compatibilities

Consider the following guidelines related to protocol requirements and compatibilities when configuring NAT.

NAT Requires IP Forwarding

IP must be configured on the router that you will configure as the NAT router. For IP forwarding, a unidirectional NAT configuration (including NAT types SDPT and N-to-1) requires that you configure either the RIP1 or RIP2 routing protocol or static routes, or a combination of these.

Bidirectional NAT requires that either RIP2 be configured on each interface in your NAT configuration that will be used for bidirectional NAT, or that you configure static routes between devices in your configuration.

OSPF and BGP Supported for Unidirectional NAT Only

In your unidirectional NAT configuration, if the NAT router will translate addresses for OSPF traffic, you must set the value of the Site Manager AS Boundary Router parameter to Yes (or in the BCC, set the value of as-boundary-router to true).

The AS boundary router parameter indicates whether or not the router functions as an AS boundary router. Only AS boundary routers can convert non-OSPF routes into OSPF routes so that they can be passed along throughout the OSPF routing domain. The router can be an AS boundary router if one or more of its interfaces is connected to a non-OSPF network (for example, RIP, BGP, or EGP).

Bidirectional NAT does not support the IP routing protocols OSPF or BGP.

ISP Mode Not Supported by NAT

NAT does not support the ISP mode feature. ISP mode is a BayRS global IP parameter that allows you to enable the BGP soloist and disable IP forwarding caches. By default, ISP mode is disabled in BayRS.

ECMP Mode Supported for Unidirectional NAT Only

Unidirectional NAT supports Equal Cost Multi-Path (ECMP) mode. ECMP is a load-balancing feature that allows IP to distribute traffic over up to five equal-cost paths to the same destination. By default, ECMP support is disabled in BayRS.

Compatibility of NAT and IPsec on a Router Interface

You can configure both unidirectional NAT and Internet Protocol Security (IPsec) on the same router interface. However, the address ranges you configure for NAT and those you configure in IPsec policy filters cannot overlap (be the same).

You can configure both IPsec and NAT using either the BCC or Site Manager. When you configure NAT and IPsec on the same router interface, NAT and IPsec operate independently and do not pass traffic to each other.

With both protocols configured on the same router interface, NAT takes precedence over IPsec. For example, if the destination address of an incoming IP packet does not match any configured NAT public address, then the packet is processed by IPsec. If the IP packet contains an address that falls within the configured range of an IPsec policy, then the packet is either protected, bypassed, or dropped. A packet with a source address not within any IPsec policy range will be dropped.

Router interfaces configured for bidirectional NAT do not support IPsec.

Special Considerations for Configuring NAT SDPT for FTP

FTP is an application-level protocol that supports the exchange of files between two hosts. FTP requires clients to satisfy security authorization in the form of a login and password. FTP is supported by all NAT types.

However, NAT SDPT support requires that you configure two SDPT translations. One of these translations is for the control connection and one is for the data connection.

NAT Config.	translation-type	private-address	public-address	private-port	public-port	protocol
1	SDPT	55.0.0.1	192.32.29.17	21	21	TCP
2	SDPT	55.0.0.1	192.32.29.17	20	20	TCP

Special Considerations for Configuring NAT SDPT for TFTP

TFTP is an application-level protocol that is a simplified version of FTP. Like FTP, TFTP transfers data files, but unlike FTP, it does not provide password protection. Also, TFTP runs on top of the connectionless datagram delivery service, UDP. TFTP is supported by all NAT types.

However, NAT SDPT support requires that you combine several translation types in your configuration. Two possible configuration scenarios are as follows:

- Configure SDPT translation “inside” an N-to-1 range, and set the N-to-1 address to be identical to the SDPT translated address.

translation-type	private-address	public-address	private-port	public-port	protocol
N-to-1	55.0.0.0/255	192.32.29.17	Not applicable	Not applicable	Not applicable
SDPT	55.0.0.1	192.32.29.17	69	69	UDP

- Configure a static translation with the same original address and translated address as the SDPT translation.

translation-type	private-address	public-address	private-port	public-port	protocol
SDPT	55.0.0.1	192.32.29.17	69	69	UDP
Static	55.0.0.1	192.32.29.17	Not applicable	Not applicable	Not applicable

Multiple Source Address Filters -- Order of Precedence for NAT Types

You can configure NAT so that a source address in a domain falls within two or more source address filters. When a domain has more than one configured source address filter, the most specific matching translation determines which type of NAT is used.

The order of translation precedence for routers configured with NAT is generally as follows:

1. SDPT
2. Static address translation
3. N-to-1 dynamic port translation
4. Dynamic address translation

When N-to-1 dynamic port translation is enabled, the source address (private interface) or the destination address (public interface) is looked up in the translation table to determine which type of translation applies to this packet. For example, for the ranges illustrated in Figure 2-13:

If a packet arrives at the interface in the private domain with a source address of:	This type of address translation occurs:
55.1.1.1	Dynamic
55.0.1.1	N-to-1 dynamic

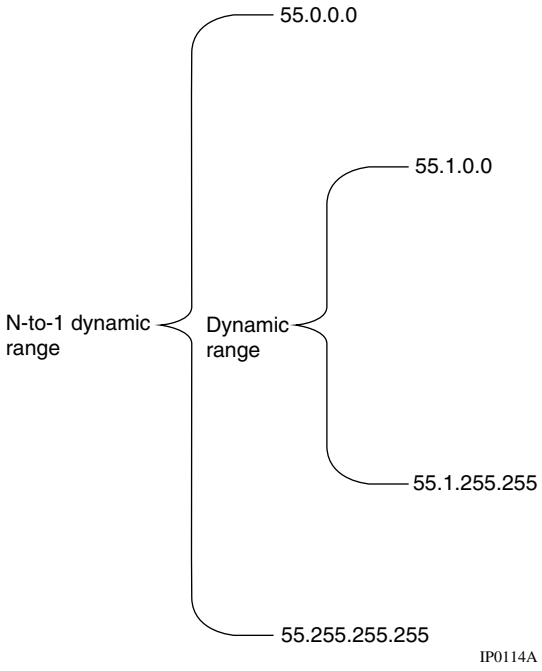


Figure 2-13. Sample Translation Types and Address Ranges

Figure 2-14 illustrates a NAT configuration in which a dynamic address range encloses an N-to-1 dynamic range, which encloses a static translation range. The static translation is the most specific. For the ranges illustrated in Figure 2-13:

If a packet arrives at the interface in the private domain with a source address of:	This type of address translation occurs:
55.1.2.3	Static
55.1.2.2	N-to-1 dynamic
55.55.1.1	Dynamic

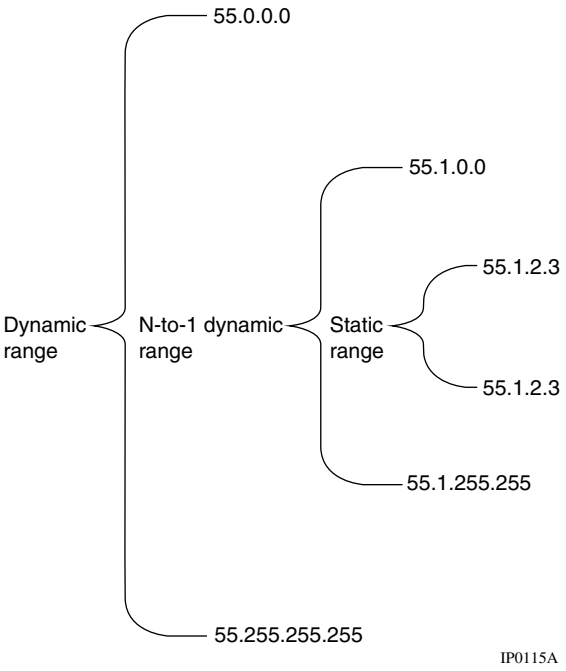


Figure 2-14. More Sample Translation Types and Address Ranges

Figure 2-15 illustrates configured NAT ranges that do not overlap. Packets with a source address that falls within any of these ranges will be translated with the translation type associated with each range. Packets falling outside these ranges are not delivered to NAT and are processed as normal IP packets.

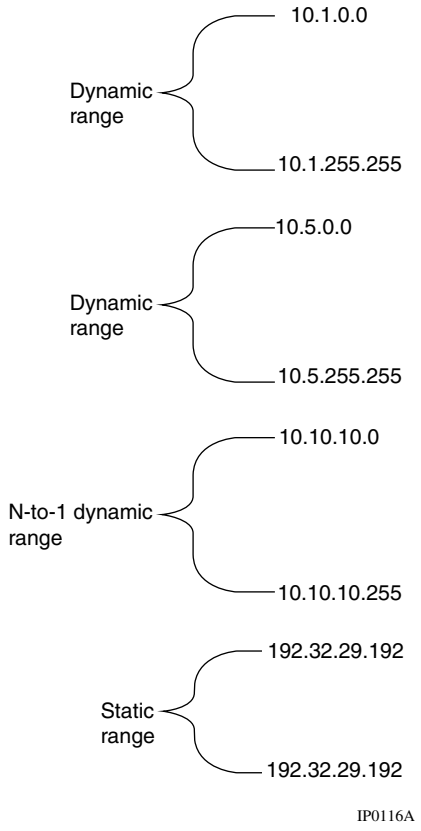


Figure 2-15. Non-overlapping Address Ranges

Internet Control Message Protocol and Message Handling

NAT automatically allows Internet Control Message Protocol (ICMP) communication and message handling. However, for N-to-1 network address translation, ICMP is supported only under the following conditions:

- When initiated from the private side of the network, N-to-1 network address translation processes ICMP communication between the following pairs. If any of these requests are received on a unidirectional *outbound* NAT interface, the NAT router logs an event message and does not process the packet.
  - -- ICMP echo request and ICMP echo response
  - -- ICMP timestamp request and ICMP timestamp response
  - -- ICMP echo mask request and ICMP echo mask response
- When initiated from either the private or public side of the network, N-to-1 translation supports the following ICMP error messages. If the "ICMP redirect error" message occurs, the NAT router logs an event message and does not process the packet.
  - -- ICMP destination unreachable
  - -- ICMP time exceeded
  - -- ICMP parameter problem
  - -- ICMP source quench

Starting NAT Services and Configuring Translations

This section provides instruction in how to start NAT and how to configure dynamic NAT, whether configuring unidirectional or bidirectional translations.

- For instructions on how to configure unidirectional NAT, see page 2-40.
- For instructions on how to configure bidirectional NAT, see page 2-50.

You can use the BCC or Site Manager to start NAT on the router. For instructions on how to start and use the BCC or Site Manager, see *Using the Bay Command Console (BCC)* or *Configuring and Managing Routers with Site Manager.*

Configuring Unidirectional NAT (Dynamic)

The following procedures explain how to start NAT services and configure unidirectional NAT, using either the BCC or Site Manager.

If you want to configure using	Go to the instructions on page
The BCC	2-40
Site Manager	2-45

Using the BCC

To use the BCC to configure a dynamic unidirectional network address translation on a router using default values for most parameters:

1. Add NAT to a router interface.
2. Specify the domain named “private.”
3. Specify a source address filter for the private domain.
4. Specify the domain named “public.”
5. Specify a translation pool.
6. Configure the private NAT interface.
7. Configure the public NAT interface.

These steps are described in the following sections.

Step 1. Add NAT to a router interface

To configure NAT on a router interface, navigate to an IP interface and add NAT (for example, **box; ethernet 2/1; ip** *<ip_address>*) and enter:

nat

When you first add NAT to a router interface, NAT is globally available on the router.

Step 2. Specify the domain named "private"

To specify the domain named "private" in NAT using the BCC, navigate to the NAT prompt (for example, **box; ip; nat**) enter:

domain private

When configuring unidirectional NAT, you must use the special domain name "private" to identify the domain that you want NAT to translate addresses from.

Step 3. Specify a source address filter for the private domain

For unidirectional NAT, the *source address filter* specifies to the router which source addresses from a single domain NAT should translate into public addresses. For dynamic NAT to work, you must configure at least one source address filter. For unidirectional NAT, the source address filter contains a range of private host addresses that NAT uses to translate into public addresses configured in a translation pool. In unidirectional NAT, you must use the special domain name "private" to configure a source address filter.

You specify a source address filter as a start address and a prefix length (from 1 through 32 decimal). The prefix length determines the number of available addresses in the source domain. For example, if the start address is 10.1.10.0 and its prefix length is 24 (255.255.255.0), then the source address filter range you specify includes addresses 10.1.10.0 to 10.1.10.255.

To configure a source address filter, navigate to the domain name prompt (for example, **box; ip; nat; domain private**) and enter:

src-filter *<start_address>/<prefix_length>*

start_address specifies the start of the IP address range available for translation. Use dotted-decimal notation.

prefix_length specifies the end of the IP address range available for translation. Use an integer from 1 through 32 that represents the number of contiguous bits in the network portion.

Example

This example shows the creation of a domain named "private" followed by the specification of a source address filter with an address range from 10.0.0.0 to 10.255.255.255. (Note that addresses 10.0.0.0 through 10.255.255.255 or address 10.0.0.0 with a prefix length of 8 is a range that is reserved for use in private networks; it is not valid on the public Internet.)

```
nat# domain private
domain/private# src-filter 10.0.0.0/8
src-filter/10.0.0.0/8/private# info
   n-to-1 0.0.0.0
   next-hop-address 0.0.0.0
   prefix-length 8
   start-address 10.0.0.0
   state enabled
   type 1-to-1
   unnumbered-circuit-name {}
   use-translation-pool outbound
src-filter/10.0.0.0/8/private#
```

The **info** command lets you see the values configured so far for this source address filter. Because only the start-address and prefix-length parameters have been configured, the rest of the values displayed by the **info** command are default values. The values 0.0.0.0 and {} mean that these parameters have not been set, so they are inactive. The type parameter is a read-only parameter that indicates whether the type of NAT being configured is static or dynamic (1-to-1) or N-to-1 (n-to-1).

The use-translation-pool parameter specifies whether the translation pool is defined for the inbound (source) or outbound (destination) domain. For unidirectional NAT, the value for use-translation-pool must be *outbound*. For bidirectional NAT, the value can be either *inbound* or *outbound* (the default).

Step 4. Specify the domain named "public"

To specify the domain named "public" in NAT using the BCC, navigate to the NAT prompt (for example, **box; ip; nat**) enter:

domain public

When configuring unidirectional NAT, you must use the special domain name "public" to identify the domain that you want NAT to translate addresses to.

Step 5. Specify a translation pool for the public domain

For unidirectional NAT, a *translation pool* is a range of IP addresses that you configure for NAT to use when dynamically translating the source addresses from IP packets matching a configured source address filter. For dynamic network address translation to work, you must configure at least one translation pool.

You specify a translation pool as a start address and a prefix length (from 1 through 32 decimal). The prefix length determines the number of available public addresses. For example, if the start address is 197.1.2.0 and its prefix length is 24 (255.255.255.0), then the translation pool range you specify includes addresses 197.1.2.0 through 197.1.2.255.

When configuring unidirectional NAT, you must use the special domain name "public" to identify the domain for the translation pool.

To configure a translation pool, navigate to the domain name prompt for public (for example, **box; ip; nat; domain public**) and enter:

trans-pool *<start_address>/<prefix_length>*

start_address specifies the start of the IP address range available for translation. Use dotted-decimal notation.

prefix_length specifies the end of the IP address range available for translation. Use an integer from 1 to 32 that represents the number of contiguous bits in the network portion.

Example

This example shows the creation of a domain named "public" followed by the specification of a translation pool with an address range from 199.1.42.0 to 199.1.42.255.

```
nat# domain public
domain/public# trans-pool 199.1.42.0/24
trans-pool/199.1.42.0/24/public# info
   prefix-length 24
   start-address 199.1.42.0
   state enabled
trans-pool/199.1.42.0/24/public#
```

The **info** command lets you see the values configured so far for this source address filter. By default, the state of the translation pool is enabled.

Step 6. Configure the NAT private interface

For unidirectional NAT, the *private interface* is the NAT router interface connected to a device in the domain specified for the source address filter. The router performs address translation only on packets from hosts included in the source address filter. Remember that when you are configuring unidirectional NAT, you must use the special domain names "private" and "public" to identify the domains that NAT translates addresses from or to.

To specify the private NAT interface between the router and the domain named "private," navigate to the appropriate IP interface prompt (for example, **box; ethernet/2/2; ip/192.132.45.3/255.255.255.0**) and enter:

nat private

Step 7. Configure the NAT public interface

For unidirectional NAT, the *public interface* is the NAT router interface connected to a device in the domain specified for the translation pool. Remember that when you are configuring unidirectional NAT, you must use the special domain names "private" and "public" to identify the domains that NAT translates addresses from or to.

IP packets arriving at the public interface from the public network are looked up and, if the source address is within the range of the source address filter, the address is translated by NAT.

To specify the public NAT interface between the router and the domain named "public," navigate to the appropriate IP interface prompt (for example, **box; ethernet/2/1; ip/192.132.22.10/255.255.255.0**) and enter:

nat public

Using Site Manager

Before you can start NAT on the router, you must configure a circuit that the protocol can use as an interface to an attached network. For instructions, see *Configuring Ethernet, FDDI, and Token Ring Services* or *Configuring WAN Line Services*.

To use Site Manager to configure a dynamic unidirectional network address translation on a router using default values for most parameters:

1. Configure NAT on the router and specify the private NAT interface.
2. Configure NAT on the public interface.
3. Configure a source address filter.
4. Configure a translation pool.

These steps are described in the following sections.

Step 1. Configure NAT on the router and specify the NAT private interface

When you first configure NAT on a router interface, NAT is available globally on the router.

For unidirectional NAT, the *private interface* is the NAT router interface connected to a device in the domain specified for the source address filter. When configuring unidirectional NAT, you must use the special domain name “private” to identify the domain that you want NAT to translate addresses from. The router performs address translation only on packets from hosts included in the source address filter.

After you have already configured IP on the router, follow these steps to configure NAT on the router and specify the private NAT interface:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the connector that you want to configure as the NAT private interface.	The Edit Connector window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
2. Click on **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens, with a check mark next to IP.
5. Click on **NAT**.	A check mark appears next to NAT.
6. Click on **OK.**	The NAT Global Configuration window opens.
7. Click on **OK** to accept the default values for NAT global parameters.	The NAT Interface Configuration window opens.
8. Click on **OK** to accept the special domain name “private.”	The Circuit Definition window displays the circuit configured with NAT.
9. Choose **File**.	The File menu opens.
10. Choose **Exit.**	You return to the Configuration Manager window.

Step 2. Configure the NAT public interface

For unidirectional NAT, the *public interface* is the NAT router interface connected to a device in the domain specified for the translation pool. When configuring unidirectional NAT, you must use the special domain name “public” to identify the domain that you want NAT to translate addresses to.

IP packets arriving at the public interface from the domain public are looked up and, if their source address matches one in the source address filter, the address is translated by NAT.

To configure the public NAT interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the connector that you want to configure as the NAT public interface.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Circuit Definition window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens.
5. Click on **NAT**, and then click on **OK**.	The NAT Interface Configuration window opens.
6. Enter **public** in the **Domain Name** parameter to specify the special domain name "public," and then click on **OK.**	You return to the Circuit Definition window.
7. Choose **File**.	The File menu opens.
8. Choose **Exit.**	You return to the Configuration Manager window.

Step 3. Configuring a source address filter

For unidirectional NAT, the *source address filter* specifies to the router which source addresses from a single domain NAT translates into public addresses. For dynamic NAT to work, you must configure at least one source address filter.

You specify a source address filter as a starting IP address and a prefix length (from 1 through 32 decimal). The prefix length determines the number of available addresses. For example, if the base address is 197.1.2.0 and its prefix length is 24 (255.255.255.0), then the address range you specify includes addresses 197.1.2.0 through 197.1.2.255.

To configure a source address filter, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic Mapping**.	The NAT Dynamic Mapping menu opens.
5. Choose **Source Address Filter.**	The NAT Source Address Filter List window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Click on **Add**.	The NAT Source Address Filter Add window opens.
7. Set the following parameters: • **IP Address** • **Prefix Length** • **Domain Name** Click on **Help** or see the parameter descriptions beginning on page A-28.	
8. Click on **OK**.	You return to the NAT Source Address Filter List window.
9. Click on **Done**.	You return to the Configuration Manager window.

Step 4. Configuring a translation pool

The *translation pool* specifies to the router which registered, public addresses NAT uses when translating addresses from the source address filter. For dynamic network address translation to work, you must configure at least one translation pool.

To configure a translation pool, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic Mapping**.	The NAT Dynamic Mapping menu opens.
5. Choose **Translation Pool.**	The NAT Translation Pool List window opens.
6. Click on **Add**.	The NAT Translation Pool Add window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
7. Set the following parameters: • **IP Address** • **Prefix Length** • **Domain Name** Click on **Help** or see the parameter descriptions beginning on page A-32.	
8. Click on **OK**.	You return to the NAT Translation Pool List window.
9. Click on **Done**.	You return to the Configuration Manager window.

Configuring Bidirectional NAT (Dynamic)

In the following bidirectional multidomain NAT configuration, a single router has interfaces to devices in two or more domains. Devices in any of these domains can initiate address translations on the NAT router. The following procedures explain how to start NAT services and configure bidirectional NAT using either the BCC or Site Manager.

If you want to configure using	Go to the instructions on page
The BCC	2-50
Site Manager	2-56

Using the BCC

To use the BCC to configure dynamic bidirectional NAT on a router using default values for most parameters, you must configure the following:

1. A DNS server with a public address on the same network as the NAT router
2. IP on router interfaces to be configured with NAT
3. RIP2 on the router IP interfaces and on each device that will use NAT

   If you do not configure RIP2 on these interfaces, you must configure IP address forwarding using static routes. The Static Nexthop parameter allows you to configure the next hop address to a domain from a NAT router interface. For more information, see "Static Nexthop Address Parameter" on page 2-99.
4. A NAT router interface to a device in each domain that will use NAT
5. DNS client on each device in the domains that will use NAT
6. DNS proxy on the router NAT interfaces
7. A source address filter for each domain that will use NAT
8. A translation pool for each domain that will use NAT

These steps are described in the following sections.

Step 1. Install DNS server on a device with a public interface to the NAT router

You must set up at least one Domain Name System (DNS) server. When configuring DNS proxy on the NAT router (step 6 below), you can specify up to three of these DNS servers as a forwarding server for address requests.

Install DNS server on a device that has a public address connection to the router that will be configured with NAT. The DNS server should also be in the same subnet as the NAT router. DNS is not part of Nortel Networks BayRS; DNS is usually provided with operating system software, such as UNIX. To set up the DNS server software, follow the instructions from the supplier of your DNS server.

Step 2. Configure IP on all router interfaces to be configured with NAT

Configure a connector and router interface with IP for each domain in your bidirectional multidomain NAT configuration. At a minimum, you must set up at least two interfaces on the NAT router, one to each of two domains that will be able to initiate address translation on the router.

To configure NAT on a router interface, you must first configure a connector and add IP to it (for example, **box; ethernet; ip**). Configuring one IP interface adds IP globally to the router. The following commands specify an Ethernet interface with IP address 23.1.1.1 and a mask of 8:

```
box# ethernet 2/2
ethernet/2/2# ip 23.1.1.1/8
ip/23.1.1.1/255.0.0.0#
```

Step 3. Configure RIP2 on the router IP interfaces and on each device that will use NAT

Configure RIP2 on the router interface to each domain in your bidirectional NAT configuration. At a minimum, you must configure two interfaces on the NAT router. In addition, you need to configure RIP2 on each device that will be sending or receiving traffic in the domains that will use bidirectional NAT.

To add RIP2 to a router interface already configured with IP, enter the command **rip**, followed by a command to specify the version. For example:

```
ip/23.1.1.1/255.0.0.0# rip
rip/23.1.1.1# version rip2
```

Step 4. Configure a NAT router interface to a device in each domain that will use NAT

Configure a NAT router interface to a device in each domain of your bidirectional NAT configuration. At a minimum, you must configure two NAT interfaces on the router. Configuring NAT on an interface also adds NAT globally on the router.

To add NAT to a router interface, navigate to the IP interface that you want to configure and enter the **nat** command, specifying a domain name. A *domain name* is a sequence of labels separated by periods. A label can contain up to 63 characters. A label must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or a hyphen. For example:

```
ip/23.1.1.1/255.0.0.0# nat domain-name domain1.com
nat/23.1.1.1# info
    domain-name domain1.com
    state enabled
```

Step 5. Configure DNS client on each device in the domains that will initiate IP traffic whose addresses will be translated by NAT

For each domain in your bidirectional multidomain NAT configuration, configure DNS client on each device that will initiate traffic requiring network address translation on the NAT router. At a minimum, this would be two devices.

When configuring your DNS client, specify the IP address of the DNS server as the domain interface to the NAT router.

For example, with IP configured globally on the router, enter the following command at the box level prompt to accept the default settings for DNS client:

```
box# dns
```

After you create and enable the DNS client on the router (the default setting), you must specify at least one DNS server with which the DNS client can communicate. To specify a DNS server, at the dns prompt enter:

name-server <*number*> **address** <*ip_address*>

number is 1, 2, or 3.

ip_address is the IP address of the DNS proxy (an interface on the NAT router).

For example, the following command sets the name-server parameter to IP address 192.32.75.9 and specifies the first DNS proxy interface for the NAT router:

```
dns# name-server 1 address 192.32.75.9
```

Note: When determining a value for the DNS client Timeout parameter, you must consider whether the DNS client contains an IP address of an interface configured with DNS proxy. If DNS client will interact with DNS proxy, be sure to set the timeout value so that it allows for the maximum time that the DNS proxy takes to cycle through each uncommunicative configured DNS server until DNS proxy encounters a server that is up. You can assign a maximum of three DNS servers for DNS proxy.

For example, if your DNS proxy is configured with two DNS servers, set the timeout for your DNS client to at least two times the value of the DNS proxy Timeout parameter and the Maximum Retransmissions parameter. If you observe an inordinate number of DNS client queries that time out internally, you may need to raise the value of the DNS client Timeouts parameter.

Step 6. Configure DNS proxy on the router NAT interfaces

Configure DNS proxy on each NAT router interface for each domain in your bidirectional multidomain NAT configuration. At a minimum, you must configure DNS proxy on two interfaces on the NAT router.

To configure DNS-proxy, navigate to the IP prompt and enter the **dns-proxy** command. The **state** command displays the default value for the state of the DNS proxy server. For example:

```
ip/23.1.1.1/255.0.0.0# dns-proxy
dns-proxy/23.1.1.1# state
   state enabled
```

For DNS proxy to work with NAT, you must also configure the DNS proxy parameters **domain-name** (specify the domain name that matches the one specified for the NAT router interface), **fwd-server1-address** (specify the address of the first DNS server for this domain; you can specify up to three forwarding servers), and **mode** (nat-translation). For example:

```
dns-proxy/23.1.1.1# domain-name domain1.com
dns-proxy/23.1.1.1# fwd-server1-address 192.165.136.45
dns-proxy/23.1.1.1# mode nat-translation
```

Here is a look at what has been configured for DNS proxy, accepting default values for all other parameters:

```
dns-proxy/23.1.1.1# info
   answer-truncation disabled
   domain-name domain1.com
   fwd-port 53
   fwd-server1-address 192.168.136.45
   fwd-server2-address 0.0.0.0
   fwd-server3-address 0.0.0.0
   max-answers-truncated 10
   max-cache-size 10
   max-queries-allowed 10
   max-retransmissions 10
   mode nat-translation
   port 53
   state enabled
   timeout 20
```

Step 7. Configure a source address filter for each domain that will use NAT

Configure one source address filter for each domain in your bidirectional multidomain NAT configuration. At a minimum, you must configure two source address filters for dynamic bidirectional NAT.

To configure a source address filter, first navigate to the NAT global prompt (for example, **box; ip; nat**) and identify the name of a domain. For example:

```
nat# domain domain1.com
```

The name must match the domain name you specified for each NAT interface configured for bidirectional NAT.

Then, enter the **src-filter** command followed by a starting IP address (specifies the start of the IP address range available for translation use) and prefix length (specifies the end of the IP address range available for translation use). Use the **info** command to display the values configured for this source address filter:

```
domain/domain1.com# src-filter 23.1.1.1/8
src-filter/23.1.1.1/8/domain1.com# info
   n-to-1 0.0.0.0
   next-hop-address 0.0.0.0
   prefix-length 8
   start-address 23.1.1.1
   state enabled
   type 1-to-1
```

```
   unnumbered-circuit-name {}
   use-translation-pool outbound
```

The type parameter is a read-only parameter that indicates whether the type of NAT is static or dynamic (1-to-1) or N-to-1 (n-to-1).

Step 8. Configure a translation pool for each domain that will use NAT

Configure one translation pool for each domain in your bidirectional multidomain NAT configuration. At a minimum, you must configure two translation pools for dynamic bidirectional NAT.

To configure a translation pool, first navigate to the NAT global prompt (for example, box; ip; nat) and identify the name of a domain. For example:

```
nat# domain domain1.com
```

The name must match the domain name you specified for each NAT interface configured for bidirectional NAT.

Then, enter the **trans-pool** command, followed by the starting IP address (specifies the start of the IP address range available for translation) and prefix length (specifies the end of the IP address range available for translation). Use the **info** command to see the values configured for this source address filter. For example, the following command sequence configures 199.1.2.0/24 as the translation pool and verifies the entry:

```
nat# domain domain1.com
domain/abc.net# trans-pool 199.1.2.0/24
trans-pool/199.1.2.0/24/domain2.net# info
   prefix-length 24
   start-address 199.1.2.0
   state enabled
```

Note: After you configure a source address filter and translation pool for each of two domains in your bidirectional NAT configuration, you can choose which translation pool to use for address translation against your source address filter. The use-translation-pool parameter (in Site Manager, the Translation Pool Selector parameter) specifies whether to use the translation pool defined for the *inbound* (source) or *outbound* (destination) domain. The default value is *outbound*.

Using Site Manager

To use Site Manager to configure a dynamic bidirectional network address translation on a router using default values for most parameters, you must configure the following:

1. A DNS server on a device with a public interface to the NAT router
2. Circuits on the router
3. IP on router interfaces to a device in each domain that will use NAT
4. RIP2 on the router IP interfaces and on each device that will use NAT

   If you do not configure RIP2 on these interfaces, you must configure IP address forwarding using static routes. The Static Nexthop parameter allows you to configure the next hop address to a domain from a NAT router interface. For more information, see "Static Nexthop Address Parameter" on page 2-99.
5. NAT on router IP/RIP2 interfaces to a device in each domain that will use NAT
6. A domain associated with each NAT router interface to be used in bidirectional multidomain NAT
7. The IP address of a DNS server to be used by DNS proxy
8. A source address filter for each domain that will use NAT
9. A translation pool for each domain that will use NAT
10. DNS client on each device in the domains that will initiate address translation

These steps are described in the following sections.

Step 1. Install DNS server on a device with a public interface to the NAT router

You must set up at least one Domain Name System (DNS) server. When configuring DNS proxy on the NAT router (step 7 below), you specify up to three of these DNS servers as a forwarding server for address requests.

Install DNS server on a device that has a public address connection to the router that will be configured with NAT. The DNS server should also be in the same subnet as the NAT router. DNS server is not part of Nortel Networks BayRS; DNS server is usually provided with operating system software, such as UNIX. To set up the DNS server software, follow the instructions from the supplier of your DNS server.

Step 2. Configure circuits on the router

You must configure at least two circuits on the router that the NAT protocol can use as interfaces from this router to devices in the domains of your bidirectional multidomain NAT configuration.

For instructions on configuring a circuit, see *Configuring Ethernet, FDDI, and Token Ring Services* or *Configuring WAN Line Services*.

Step 3. Configure IP on the router interfaces

Configure two router interfaces with IP, as follows:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, select **IP**. Then click on **OK**.	The IP Configuration window opens.
2. Set the following parameters: • **IP Address** • **Subnet Mask** • **Transmit Bcast Addr** • **UnNumbered Assoc Address** Click on **Help** or see the parameter descriptions in *Configuring IP, ARP, RARP, RIP, and OSPF Services*.	When you have successfully configured a circuit, the Select Protocols window opens.
3. Click on **OK**.	Site Manager prompts you to enable TFTP on the router.
4. Click on **Yes** to enable TFTP. Otherwise, click on **No**.	You return to the Configuration Manager window.

Step 4. Configure RIP2 on the router IP interfaces and on each device that will use NAT

Configure RIP2 on the IP router interface to each domain in your bidirectional multidomain NAT configuration. At a minimum, you must configure two IP/RIP2 interfaces on the NAT router. In addition, you need to configure RIP2 on each device that will be sending or receiving traffic in the domains that will use bidirectional NAT.

To add RIP2 to an existing IP interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the connector to which you want to add RIP services.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens.
5. Click on **RIP**.	Site Manager highlights the selection.
6. Click on **OK**.	You return to the Circuit Definition window.
7. From the **Protocols** menu choose **Edit IP**.	The Edit IP menu opens.
8. Choose **RIP Interfaces.**	The IP RIP Interface Configuration window opens, with the IP RIP circuits listed in the list window.
9. Scroll down to the Rip Mode parameter, click in the text box, then click on the Values button.	The Values Selection window opens, with the available values for this parameter.
10. Click on **RIP2**.	
11. Click on **OK**.	RIP2 appears in the Rip Mode text box with a different color background.
12. Click on **Apply**.	As the setting is applied, the background color of the RIP2 value matches the rest of the values.
13. Click on **Done**.	You return to the Circuit Definition window.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
14. Choose **File**.	The File menu opens.
15. Choose **Exit**.	You return to the Configuration Manager window.

Steps 5, 6, 7: Configure NAT on an interface, specify a domain name, and identify a DNS server for NAT router DNS proxy

Configure a NAT router interface to a device in each domain of your bidirectional multidomain NAT configuration. At a minimum, you must configure two NAT interfaces on the router. Configuring NAT on the first router interface adds NAT globally to the router.

For each IP/RIP2 interface you must configure, follow these steps to configure NAT on the router, specify the domain name associated with the interface, and identify an IP address as the DNS server for DNS proxy:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the connector that you want to configure as the NAT private interface.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens, with a check mark next to IP.
5. Click on **NAT**.	A check mark appears next to NAT.
6. Click on **OK.**	The NAT Global Configuration window opens.
7. Click on **OK** to accept the default values for NAT global parameters.	The NAT Interface Configuration window opens.
8. In the **Domain Name** field, enter the name of one of the domains for which NAT will be translating addresses from or to.	Site Manager prompts you whether to install DNS proxy now.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
9. Click on **Yes.***	The DNS Proxy Record window opens, with default entries in the Domain Name and Proxy Mode fields.
10. Specify an address for DNS Server 1, then click on **OK**.	The Circuit Definition window displays the circuit configured with NAT.
11. Choose **File**.	The File menu opens.
12. Choose **Exit.**	You return to the Configuration Manager window.

* If, for some reason, you decide not to configure DNS proxy at this point, see the instructions for configuring DNS proxy in *Configuring IP Utilities*. Specific to dynamic bidirectional NAT, you must set values for Domain Name (the name of one of your domains to be used in bidirectional NAT translations), Proxy Mode (set to *NAT Translation*), and you must specify the IP address of at least one, and up to three, DNS servers. DNS proxy on the NAT router communicates with this DNS server for address information.

Step 8: Configure a source address filter for each domain that will use NAT

Configure one source address filter for each domain in your bidirectional multidomain NAT configuration. At a minimum, you should configure two source address filters for dynamic bidirectional NAT.

You specify a source address filter as a starting IP address and a prefix length (from 1 through 32 decimal). The prefix length determines the number of available addresses. For example, if the base address is 197.1.2.0 and its prefix length is 24 (255.255.255.0), then the address range you specify includes addresses 197.1.2.0 through 197.1.2.255. The addresses in the source address filter are used by the router to determine which source addresses get translated by NAT.

To configure a source address filter, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic Mapping**.	The NAT Dynamic menu opens.
5. Choose **Source Address Filter.**	The NAT Source Address Filter List window opens.
6. Click on **Add**.	The NAT Source Address Filter Add window opens.
7. Set the following parameters: • **IP Address** • **Prefix Length** • **Domain Name** Click on **Help** or see the parameter descriptions beginning on page A-28.	
8. Click on **OK**.	You return to the NAT Source Address Filter List window.
9. Click on **Done**.	You return to the Configuration Manager window.

Step 9. Configuring a translation pool for each domain that will use NAT

Configure one translation pool for each domain in your bidirectional multidomain NAT configuration. At a minimum, you should configure two translation pools for dynamic bidirectional NAT.

The IP Address parameter lets you specify the start of the IP address range available for translation, the Prefix Length parameter specifies the end of the IP address range available for translation, and the value you supply for the Domain Name parameter must match the domain name you specified for each respective NAT interface configured for bidirectional NAT. The addresses in the translation pool are used by the NAT router to translate any source addresses that match the addresses specified in the source address filter.

To configure a translation pool, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic Mapping**.	The NAT Dynamic menu opens.
5. Choose **Translation Pool.**	The NAT Translation Pool List window opens.
6. Click on **Add**.	The NAT Translation Pool Add window opens.
7. Set the following parameters: • **IP Address** • **Prefix Length** • **Domain Name*** Click on **Help** or see the parameter descriptions beginning on page A-32.	
8. Click on **OK**.	You return to the NAT Translation Pool List window.
9. Click on **Done**.	You return to the Configuration Manager window.

* You must change Domain Name from public or private, which are applicable values only for unidirectional NAT.

Note: After you configure a source address filter and translation pool for each of two domains in your bidirectional NAT configuration, you can choose which translation pool to use for address translation against your source address filter. The Translation Pool Selector parameter (in the BCC, the use-translation-pool parameter) specifies whether to use the translation pool defined for the *inbound* (source) or *outbound* (destination) domain. The default the value is *outbound*.

Step 10. Configure DNS client on each device in the domains that will initiate address translation on the NAT router

For each domain in your bidirectional multidomain NAT configuration, configure DNS client on each device that will initiate traffic requiring network address translation on the NAT router. At a minimum, this would be two devices.

Note: When determining a value for the DNS client Timeout parameter, you must consider whether the DNS client contains an IP address of an interface configured with DNS proxy. If DNS client will interact with DNS proxy, be sure to set the timeout value so that it allows for the maximum time that the DNS proxy takes to cycle through each uncommunicative configured DNS server until DNS proxy encounters a server that is up. You can assign a maximum of three DNS servers for DNS proxy.

For example, if your DNS proxy is configured with two DNS servers, set the timeout for your DNS client to at least two times the value of the DNS proxy Timeout parameter and the Maximum Retransmissions parameter. If you observe an inordinate number of DNS client queries that time out internally, you may need to raise the value of the DNS client Timeouts parameter.

To create and enable the DNS client, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **Global Protocols**.	The Global Protocols menu opens.
3. Choose **DNS**.	The DNS menu opens.
4. Choose **Create DNS Client**.	The DNS Configuration window opens.
5. Click on **OK**.	You return to the Configuration Manager window.

Where to Go Next

The instructions in "Starting NAT Services and Configuring Translations" are the minimal instructions required to enable NAT operation with dynamic address translation on your router. From this point, you can customize NAT operation on your router or configure other types of address translation. Use the following table to determine where to go next:

If you want to	Go to
Change default settings for NAT global parameters	"Customizing NAT Global Parameters" on page 2-65
Change default settings for NAT interface parameters	"Customizing a NAT Interface" on page 2-74
Configure static address translation	"Configuring NAT Static Address Translation" on page 2-80
Configure a static unidirectional translation	"Adding a Static Unidirectional Address Mapping" on page 2-81
Configure a static bidirectional translation	"Adding a Static Bidirectional Address Mapping" on page 2-84
Configure static address and static port translation (SDPT type)	"Adding an SDPT Address and Port Mapping" on page 2-89
Configure dynamic address translation	"Configuring NAT Dynamic Address Translation" on page 2-95
Configure static address and dynamic port translation (N-to-1 type)	"Configuring NAT N-to-1 Translation" on page 2-113

Customizing NAT Global Parameters

To customize the way NAT operates on a router, modify NAT global attributes as described in the following sections:

Topic	Page
Enabling and Disabling NAT on the Router	2-66
Configuring the Soloist Slot Mask	2-67
Logging NAT Messages	2-69
Enabling and Disabling the Dynamic Mapping Aging Timer	2-71
Configuring the Dynamic Mapping Timeout Value	2-72

Enabling and Disabling NAT on the Router

When you first configure any router interface with NAT, NAT becomes globally enabled for the router. Use the BCC or Site Manager to enable or disable NAT on the router.

Using the BCC

To enable or disable NAT on the router, navigate to the global NAT prompt (for example, **box; ip; nat**) and enter:

state *<state>*

state is one of the following:

enabled (default)
disabled

Using Site Manager

To enable or disable NAT on the router, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Global**.	The NAT Global Configuration window opens.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-8.	
6. Click on **OK**.	You return to the Configuration Manager window.

Configuring the Soloist Slot Mask

By default, the router uses any available slot for the NAT soloist.

Note: On a BLN® router, you cannot configure the NAT soloist to run on the first slot. On a BCN® router, you cannot configure the NAT soloist on slot 7.

Use the BCC or Site Manager to specify which slots can run as the NAT soloist.

Using the BCC

To specify the slots on which NAT can run as a soloist, navigate to the global NAT prompt (for example, **box; ip; nat**) and enter:

slot-mask *<slot>*

slot can be one or more slots from 1 through 14, depending on the number of slots available on your type of router. If you enter more than one slot number, you must enclose the numbers in braces or in quotation marks. By default, all slots ("all-slots") are selected.

For example, the following command sequence selects slots 1 and 5 as the preferred NAT soloist slots and verifies the change:

```
nat# slot-mask {1 5}
nat# info
    slot-mask {1 5}
    log-mask none
    timeout enabled
    timeout-max 3600
    state enabled
```

Using Site Manager

To specify the slots on which NAT can run as a soloist, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Global**.	The NAT Base Group Record window opens.
5. Click on the **Soloist Slot Mask** field.	
6. Click on **Values**.	Site Manager displays a list of slots.
7. Choose the slots that you want to specify as available to run NAT as a soloist. Click on **Help** or see the parameter description on page A-8.	Site Manager displays the binary values that correspond to your slot selections in the Soloist Slot Mask field. The left-most bit represents the slot with the lowest number. For example, if a router has five slots, and you choose slots 3 and 5, the binary value 00101 appears in the Soloist Slot Mask field.
8. Click on **OK**.	You return to the Configuration Manager window.

Logging NAT Messages

By default, BayRS does not log NAT messages. You can enable the logging of messages by specifying the types of messages that the router should log. Table 2-3 lists the message types that can be logged by NAT software. If you enable logging, the change is effective immediately (if there are any messages to be logged).

Table 2-3. NAT Log Message Types

Message Type	Definition	Bit Position	Hex Value	BCC Keyword (mask_keyword)
NAT_DBG_MIB_LOG	MIB-related events	0	0x00000001	mib
NAT_DBG_IP_LOG	Debug events at IP level	1	0x00000002	ip
NAT_DBG_FWD_LOG	Forwarding events	2	0x00000004	forwarding
NAT_DBG_MAPPING_LOG	Translation table events	3	0x00000008	mapping
NAT_DBG_AGING_LOG	Aging level events	4	0x00000010	aging

Use the BCC or Site Manager to specify whether or not to log NAT messages.

Using the BCC

To specify the types of log messages that are reported by NAT software, navigate to the global NAT prompt (for example, **box; ip; nat**) and enter:

log-mask *<mask_keyword>*

mask_keyword can be one or more keywords representing the log type (see Table 2-3). If you enter more than one keyword, you must enclose them in braces or in quotation marks. The default is none.

For example, the following command enables the logging of NAT event messages with the logging levels NAT_DBG_MIB_LOG and NAT_DBG_IP_LOG:

```
nat# log-mask {mib ip}
nat#
```

To select all log messages, enter:

log-mask all

To specify that no NAT event messages are logged, enter:

log-mask none

Using Site Manager

To specify the types of log messages that are reported by NAT software, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Global**.	The NAT Global Configuration window opens.
5. To set the **Log Mask** parameter, click on the Log Mask field, then click on **Values**, and click on the message types that you want to log. Click on **Help** or see the parameter description on page A-9.	
6. Click on **OK**.	Site Manager displays the binary values that correspond to your log message type selections in the Log Mask field.
7. Click on **OK**.	You return to the Configuration Manager window.

Enabling and Disabling the Dynamic Mapping Aging Timer

By default, the router deletes expired dynamic NAT translation table entries. If there have been no translated packets for a specific dynamic address mapping by the time the value of the BCC timeout-max parameter (in Site Manager, the Mapping Timeout parameter) is reached, NAT software removes the entry from the dynamic translation entry list, freeing the address for another mapping.

Note: A static address translation mapping does not time out as dynamic translations do, but remains configured until you disable or delete it. For instructions, see "Disabling and Reenabling a Static Address Mapping" on page 2-92 or "Deleting a Static Address Mapping" on page 2-93.

Use the BCC or Site Manager to enable or disable the dynamic mapping aging timer.

Using the BCC

To enable or disable the mapping aging timer, navigate to the global NAT prompt (for example, **box; ip; nat**) and enter:

timeout *<state>*

state is one of the following:

enabled (default)
disabled

Using Site Manager

To change the mapping aging status, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Global**.	The NAT Global Configuration window opens.
5. Set the **Mapping Aging** parameter. Click on **Help** or see the parameter description on page A-9.	
6. Click on **OK**.	You return to the Configuration Manager window.

Configuring the Dynamic Mapping Timeout Value

A NAT dynamic mapping (translation entry) has an associated "last-use" value that increases each second that it is unused. Every time the entry is used, its last-use value is reset to 0. If the BCC timeout parameter (or the Mapping Aging parameter in Site Manager) is enabled, and the last-use value meets or exceeds the timeout value, then the translation is deleted and the address is available for reuse.

Nortel Networks recommends that you accept the default timeout value of 3600 seconds (1 hour). If you set the timeout value too low, the timer expires before NAT software can process the next packet. You can specify a value from 0 through 2,147,483,647 seconds (approximately 68 years).

Note: If you disable or delete a translation pool or change the value of the BCC use-translation-pool parameter (in Site Manager, the Translation Pool Selector parameter) to *inbound*, the dynamic translations in the NAT mapping table do not instantly disappear. To force the removal of dynamic translation entries based on the former translation pool, modify the value of the BCC timeout-max parameter (in Site Manager, the Mapping Timeout parameter).

Use the BCC or Site Manager to configure the value of the dynamic mapping timeout.

Using the BCC

To configure the timeout period for a dynamic translation entry, navigate to the global NAT prompt (for example, **box; ip; nat**) and enter:

timeout-max *<timeout>*

timeout is the duration of the timeout period in seconds.

For example, the following command configures a timeout period of 7200 seconds (2 hours):

```
nat# timeout-max 7200
nat#
```

Using Site Manager

To configure the timeout period for a dynamic translation entry, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Global**.	The NAT Global Configuration window opens.
5. Set the **Mapping Timeout (secs)** parameter. Click on **Help** or see the parameter description on page A-10.	
6. Click on **OK**.	You return to the Configuration Manager window.

Customizing a NAT Interface

This section includes the following topics:

Topic	Page
Adding NAT to an Interface	2-74
Disabling and Reenabling NAT on an Interface	2-77
Deleting NAT from an Interface	2-79

Adding NAT to an Interface

Use the BCC or Site Manager to add NAT to a router interface configured with IP. For instructions on configuring IP, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

Using the BCC

To add NAT to an IP interface, navigate to an IP interface-specific prompt (for example, **box; ethernet/13/1; ip/1.2.3.4/255.0.0.0**) and enter:

nat

For example, the following command sequence adds NAT to IP interface 123.6.31.4/255.0.0.0 and displays default NAT interface parameters:

```
ip/123.6.31.4/255.0.0.0# nat
nat/123.6.31.4# info
    type local
    state enabled
```

Using Site Manager

To add NAT to a router IP interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the connector to which you want to add NAT services.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens.
5. Click on **NAT**, and then click on **OK**.	If this is the first NAT interface on the router, the NAT Global Configuration window opens. Otherwise, the NAT Interface Configuration window opens. If this happens, you can skip the next step.
6. Click on **OK** to accept the default values for NAT global parameters.	The NAT Interface Configuration window opens, with “private” as the default in the Domain Name field.
7. This step varies, depending on whether you are configuring unidirectional NAT or bidirectional NAT: • If you are configuring an interface for unidirectional NAT, then click on **OK** to accept the special domain name, “private.” Go to Step 10. • If you are configuring an interface for bidirectional NAT, enter the appropriate domain name and click on **OK**.	 The Circuit Definition window displays the circuit configured with NAT. Site Manager asks whether to configure DNS Proxy now.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
8. Click on **Yes** or click on **No**:	
• If you click on **Yes,** specify an address for DNS Server 1, then click on **OK**.	The DNS Proxy Record window opens, with default entries for the Domain Name and Proxy Mode fields. The Circuit Definition window displays the circuit configured with NAT.
• If you click on **No**, then click on **OK**.	Site Manager displays the message, "Dynamic translation will NOT function until the DNS proxy for this interface is configured." The Circuit Definition window displays the circuit configured with NAT.
9. Choose **File**.	The File menu opens.
10. Choose **Exit**.	You return to the Configuration Manager window.

Disabling and Reenabling NAT on an Interface

When you add NAT to a router interface, NAT is enabled by default. Use the BCC or Site Manager to disable or reenable NAT on an interface.

Using the BCC

To disable or reenable NAT on an interface, navigate to the NAT interface prompt (for example, **box; ethernet/2/1; ip/121.66.37.4/255.0.0.0; nat)** and enter:

state *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command sequence disables NAT on IP interface 121.66.37.4/255.0.0.0 and verifies the change:

```
ip/121.66.37.4/255.0.0.0# nat
nat/121.66.37.4#  state disabled
nat/121.66.37.4# info
    state disabled
```

Using Site Manager

To disable or reenable NAT on an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Interface**.	The NAT Interface List window opens.
5. Select the interface that you want to enable or disable from the list.	
6. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-11.	
7. Click on **Done**.	You return to the Configuration Manager window.

Deleting NAT from an Interface

When you delete NAT from the last NAT-configured interface, global NAT is also deleted from the router. Use the BCC or Site Manager to delete NAT from an IP interface.

Using the BCC

To delete NAT from an interface, navigate to the NAT interface prompt (for example, **box; ethernet/13/1; ip/1.2.3.4/255.0.0.0; nat/1.2.3.4**) and enter:

delete

For example, the following command deletes NAT from IP interface 121.66.37.4/255.0.0.0:

```
ip/121.66.37.4/255.0.0.0# nat
nat/121.66.37.4# delete
ip/121.66.37.4/255.0.0.0#
```

Using Site Manager

To delete NAT from an interface, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the connector from which you want to delete NAT services.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens. The NAT button is checked to show that NAT is enabled on the circuit.
5. Click on **NAT**.	The check mark disappears.
6. Click on **OK**.	You return to the Circuit Definition window.
7. Choose **File**.	The File menu opens.
8. Choose **Exit**.	You return to the Configuration Manager window.

Configuring NAT Static Address Translation

Static address mapping entries must be unique; two static mapping entries cannot share either the same original IP address or the same translated IP address. Make sure that the address translations you assign in static mode for one NAT address domain do not overlap in real time with any translation address ranges in another NAT address domain, such as those configured for dynamic translations. If you try to configure a static address mapping using a public IP address that is currently being used for a dynamic translation, you receive an error message.

You can configure the following types of static network address translations:

- Unidirectional -- The mapping of addresses is from domain “private” to domain “public.”
- Bidirectional -- The mapping of addresses is between two or more domains. Translations can be initiated from a host in any domain that you specify as connected to the NAT router. The DNS proxy server must be configured on the NAT router.
- SDPT -- The mapping of IP addresses and port numbers are from domain “private” to domain “public.” Once configured, the NAT translation is initiated from the public domain into the NAT router. SDPT is a type of unidirectional NAT that is applicable only for TCP or UDP traffic.

For instructions on how to configure static address translation, see:

Topic	Page
Adding a Static Unidirectional Address Mapping	2-81
Adding a Static Bidirectional Address Mapping	2-84
Adding an SDPT Address and Port Mapping	2-89
Disabling and Reenabling a Static Address Mapping	2-92
Deleting a Static Address Mapping	2-93

Adding a Static Unidirectional Address Mapping

To add a static unidirectional mapping, you must do the following:

1. **Configure NAT on the router. For instructions, see "Adding NAT to an Interface" on page 2-74.**
2. **Configure a private and a public interface on the NAT router. For instructions:**

If you want to configure using	See
The BCC	"Step 6. Configure the NAT private interface" on page 2-44 and "Step 7. Configure the NAT public interface" on page 2-44
Site Manager	"Step 1. Configure NAT on the router and specify the NAT private interface" on page 2-45 and "Step 2. Configure the NAT public interface" on page 2-46

3. **Configure RIP1, RIP2, or static routes on the NAT router interfaces. You must also configure RIP or static routes on each device in the domain "private" that passes traffic into the NAT router for address translation and on each device in the domain "public" that passes traffic with translated addresses out of the NAT router. For instructions on configuring RIP, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.**
4. **Specify a static mapping of the original, private address to the translated, public address. Instructions follow.**
5. **For the BCC, specify the special domain "private" (*in-domain-name*) and the special domain "public" (*out-domain-name*) that respectively contain the original and translated static map addresses. Instructions follow.**

Similar to static bidirectional mapping, you map a single address to another single address. The difference is that for static unidirectional NAT, the matching source address of an IP packet originates from a device in the domain named "private"; for static bidirectional NAT the translation can be initiated from a device in any domain and both the source and destination addresses are translated for the IP packet.

Optionally, you can specify either a static next hop or an unnumbered circuit name (or neither if these) for your static unidirectional mapping:

- *Static nexthop*
  Use the Static Nexthop parameter in Site Manager (next-hop-address, in the BCC) to specify statically the next hop IP address of a device with an interface to the NAT router, when this interface does not have RIP configured. The device at the static next hop address you specify makes route information available to the NAT router when handling IP traffic. If you set this parameter, then you do not have to configure RIP on the outgoing NAT interface.
- *Unnumbered circuit name*
  If you have any unnumbered circuits bordering your NAT router, you may need to configure the unnumbered circuit name parameter.

Use the BCC or Site Manager to add a unidirectional (non-SDPT or N-to-1) static address mapping.

Using the BCC

To add a unidirectional static address mapping, navigate to the prompt for the NAT special domain "private" (for example, **box; ip; nat; domain private**) and enter:

static-map *<original_address>/<translated_address>/<out_domain_name>*

original_address is the address of a host in your private network. Enter the address in dotted-decimal notation.

translated_address is the translation address that you want to map to the original address. Enter a valid IP address in dotted-decimal notation.

out_domain_name for unidirectional NAT must be the special domain name "public."

For example, to statically map the original address 10.1.1.1 to be translated to the public IP address of 199.1.42.200 for the domain "private," you would enter the following:

```
nat# domain private
domain/private# static-map 10.1.1.1/199.1.42.200/public
static-map/10.1.1.1/199.1.42.200/private# info
   in-domain-name private
   next-hop-address 0.0.0.0
   original-address 10.1.1.1
```

```
out-domain-name public
state enabled
translated-address 199.1.42.200
unnumbered-circuit-name {}
```

The results of the **info** command display default values for all other parameters that have not been set. The values 0.0.0.0 and {} (empty set) mean that this parameter is inactive.

Using Site Manager

To add a unidirectional static address mapping, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Static Mapping**.	The NAT Static Translation List window opens.
5. Click on **Add**.	The Add Static Translation Type window opens.
6. Click on **Unidirectional,** and then click on **OK**.	The Unidirectional Translation Add window opens.
7. Set the following parameters (Static Nexthop and Unnumbered CCT Name are optional): • **Private Address** • **Public Address** • **Static Nexthop** • **Unnumbered CCT Name** Click on **Help** or see the parameter descriptions beginning on page A-22.	
8. Click on **OK**.	You return to the NAT Static Translation List window, and the new static mapping pair appears in the display list.
9. Click on **Done**.	You return to the Configuration Manager window.

Adding a Static Bidirectional Address Mapping

For static bidirectional NAT, you must do the following:

1. **Configure NAT on the router. For instructions, see "Adding NAT to an Interface" on page 2-74.**
2. **Configure each NAT interface to a domain to be used in the bidirectional mapping. These interfaces must be public, registered IP addresses.**

If you want to configure using	See
The BCC	"Step 4. Configure a NAT router interface to a device in each domain that will use NAT" on page 2-52
Site Manager	"Step 3. Configure IP on the router interfaces" on page 2-57

3. **Configure RIP2 on each interface that will be used for bidirectional NAT, or you can configure static routes between devices.**
   - -- For instructions on configuring RIP2 using the BCC, see "Step 3. Configure RIP2 on the router IP interfaces and on each device that will use NAT" on page 2-51.
   - -- For instructions on configuring RIP2 using Site Manager, see "Step 4. Configure RIP2 on the router IP interfaces and on each device that will use NAT" on page 2-58.
   - -- For more information about RIP, see *Configuring IP, ARP, RARP, RIP, and OSPF Services.*
4. **Specify a source domain (in the BCC, *in-domain-name*) and a destination domain (in the BCC, *out-domain-name*). These domain names can be any domain name except for private and public, which are reserved for unidirectional NAT. Instructions follow.**
5. **Specify a static mapping of the original, private address mapped to the translated, public address. Instructions follow.**

Similar to static unidirectional mapping, you are mapping a single address to another single address. However, with static bidirectional NAT the translation is initiated from a host in either domain (rather than the translation being initiated only from a host in the private domain, as occurs with unidirectional NAT). For this reason, at a minimum you must configure static mappings in two different domains.

The configuration of DNS proxy on the NAT router, required for dynamic bidirectional NAT, is optional when configuring static bidirectional NAT.

If you want to configure static bidirectional NAT	**For each translation, you must statically map on the NAT router**
Without DNS proxy configured on the NAT router	An original address (in Site Manager, known as the Private Address) to a translated address (in Site Manager, this is the Public Address). You must also specify a destination or “out” domain name.
With DNS proxy configured on the NAT router	Two mappings of an original address to a translated address. The first mapping is as described above. For the second mapping, use the same original address, but specify a unique translation address and specify the original domain name as the destination domain name.

For more detail, see “Examples of Configuring Static Bidirectional NAT to Work with or Independent of DNS Proxy on the NAT Router” on page 2-87.

Optionally, use the Static Nexthop parameter in Site Manager (next-hop-address, in the BCC) to specify statically the next hop IP address of a device with an interface to the NAT router, when this interface does not have RIP configured. The device at the static next hop address you specify makes route information available to the NAT router when handling IP traffic. If you set this parameter, then you do not have to configure RIP on the NAT interface.

Use the BCC or Site Manager to add a bidirectional static address mapping.

Using the BCC

To add a bidirectional static address mapping on the NAT router, navigate to the prompt for the specific NAT in domain, meaning the domain that NAT will translate addresses from (for example, **box; ip; nat; domain abc.com**) and enter:

static-map *<original_address>/<translated_address>/<out_domain_name>*

original_address is the address of a host in the source network, inbound to the NAT router. Enter the address in dotted-decimal notation.

translated_address is the address in the destination network (outbound from the NAT router) that you want to map to the original address. Enter a valid IP address in dotted-decimal notation.

out_domain_name for bidirectional NAT can be any valid domain name (acceptable characters include alphanumeric characters, a hyphen, and a period. A domain name must begin with a letter.), except for "private" and "public," which are reserved for use with unidirectional NAT.

For example, to statically map the original address 10.1.3.1 in domain abc.net to be translated to the IP address of 194.1.63.20 for the domain xyz.com you would enter the following:

```
nat# domain abc.net
domain/abc.net# static-map 10.1.3.1/194.1.63.20/xyz.com
static-map/10.1.3.1/194.1.63.20/xyz.com# info
   in-domain-name abc.com
   next-hop-address 0.0.0.0
   original-address 10.1.3.1
   out-domain-name xyz.com
   state enabled
   translated-address 194.1.63.20
   unnumbered-circuit-name {}
```

The results of the **info** command display default values for all other parameters that have not been set. The values 0.0.0.0 and {} mean that this parameter is inactive.

Examples of Configuring Static Bidirectional NAT to Work with or Independent of DNS Proxy on the NAT Router

The following is an example of a simple static mapping without configuring DNS proxy on the NAT router. Navigate to the domain1.com domain context (for example, **box; ip; nat; domain domain1.com**), then map original IP address 29.1.1.1 to the translation address 123.5.5.5, with domain2.com as the destination or "out" (of the NAT router) domain.

```
domain domain1.com
static-map 29.1.1.1/123.5.5.5/domain2.com
```

You would also make a similar mapping from a second domain, as shown for domain2.com.

```
domain domain2.com
static-map 38.2.2.2/117.4.4.4/domain1.com
```

However, when configuring static bidirectional with DNS proxy on the NAT router, you must configure a second translation for each domain. For example:

```
domain domain1.com
static-map 29.1.1.1/123.5.5.5/domain2.com
static-map 29.1.1.1/123.5.5.6/domain1.com

domain domain2.com
static-map 38.2.2.2/117.4.4.4/domain1.com
static-map 38.2.2.2/117.4.4.5/domain2.com
```

The same principles would apply for configuring using Site Manager.

Using Site Manager

To add a bidirectional static address mapping, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Static Mapping**.	The NAT Static Translation List window opens.
5. Click on **Add**.	The Add Static Translation Type window opens.
6. Click on **Bidirectional,** and then click on **OK**.	The Bidirectional Translation Add window opens.
7. Set the following parameters (Static Nexthop is optional): • **Private Address** • **Source Domain** • **Public Address** • **Destination Domain** • **Static Nexthop** Click on **Help** or see the parameter descriptions beginning on page A-17.	
8. Click on **OK**.	You return to the NAT Static Translation List window, and the new static mapping pair appears in the display list.
9. Click on **Done**.	You return to the Configuration Manager window.

Adding an SDPT Address and Port Mapping

To configure NAT SDPT you statically map the addresses and ports from the private domain to the public domain. However, once configured, the NAT router translation will be initiated from a host in the public domain. Remember that SDPT translation is applicable for TCP or UDP traffic only.

NAT SDPT requires that RIP1, RIP2, or static routes be configured on the NAT router and configured on each device in the domain "private" that will be passing traffic into the NAT router for address translation and each device in the domain "public" that receives a translated source address from the NAT router. For more information, see *Configuring IP, ARP, RARP, RIP and OSPF Services*.

For static destination port translation mapping, you must complete these tasks (instructions follow):

1. **Specify the special domain "private" (*in-domain-name*, in the BCC) and the special domain "public" (*out-domain-name*, in the BCC) that contain the original and translated static map addresses, respectively.**
2. **Specify a static mapping of an IP address in the special domain "private" to one public address in the special domain "public."**
3. **Specify a static mapping of one port number in the special domain "private" to a port number in the special domain "public."**
4. **Specify the protocol, whether TCP or UDP, that the traffic application will use.**
5. **Configure the router with a NAT interface to the domain named "private" and another interface to the domain named "public."**

Use the BCC or Site Manager to add a NAT SDPT static mapping.

Using the BCC

To add an SDPT static address mapping, navigate to the prompt for the NAT special domain "private" as the *<in-domain-name>* (for example, **box; ip; nat domain private**) and enter:

static-sdpt *<original_address>/<translated_address>/<protocol>/<original_port>/<translated_port>/<out_domain_name>*

original_address is the address of a host in your private network. Enter the address in dotted-decimal notation.

translated_address is the public address that you want to map to the original address. Enter a valid IP address in dotted-decimal notation.

protocol is the protocol for the application traffic, whether TCP or UDP.

original_port specifies the public TCP or UDP port number of a host in the domain "private."

translated_port specifies the private TCP or UDP port number of a host in the domain "public."

out_domain_name for SDPT must be the special domain name "public."

This example illustrates how to statically map the original address 21.1.1.1 in the domain "private" to be translated to the public IP address of 195.2.34.167, and specify the TCP protocol with port 23 as the (original) port in the private domain and port 8023 as the (translated) port in the public domain.

First, navigate to the NAT global prompt (**box; ip; nat**) and identify the domain named "private" for which you will be providing SDPT mapping information. Then, enter your SDPT mapping:

```
nat# domain private
domain/private# static-sdpt 21.1.1.1/195.2.34.167/tcp/23/8023/public
static-sdpt/21.1.1.1/195.2.34.167/tcp/23/23/public# info
   state enabled
   original-address 21.1.1.1
   translated-address 195.2.34.167
   in-domain-name private
   out-domain-name public
   protocol tcp
   original-port 23
   translated-port 8023
```

For this SDPT mapping to be complete, you also must configure the NAT router interfaces to the domain named "private" and to the domain named "public." For example:

```
box# ethernet 2/1
ethernet2/1# ip 10.1.2.3/8
ip/10.1.2.3/255.0.0.0# nat domain-name private
nat/10.1.2.3# back
ip/10.1.2.3/255.0.0.0# back
ethernet2/1# back
box# ethernet 2/2
ethernet2/2# ip 192.1.2.3/8
```

```
ip/192.1.2.3/255.0.0.0# nat domain-name public
nat/192.1.2.3#
```

Using Site Manager

Before you complete the following steps, you must configure NAT globally on the router and specify both a NAT private and a NAT public interface. For instructions on using Site Manager, see:

- "Step 1. Configure NAT on the router and specify the NAT private interface" on page 2-45.
- "Step 2. Configure the NAT public interface" on page 2-46.

To add an SDPT static address mapping, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Static Mapping**.	The NAT Static Translation List window opens.
5. Click on **Add**.	The Add Static Translation Type window opens.
6. Click on **SDPT**, and then click on **OK**.	The Bidirectional Translation Add window opens.
7. Set the following parameters: • **Private Address** • **Private Port** • **Public Address** • **Public Port** • **Protocol** Click on **Help** or see the parameter descriptions beginning on page A-20.	
8. Click on **OK**.	You return to the NAT Static Translation List window, and the new static mapping pair appears in the display list.
9. Click on **Done**.	You return to the Configuration Manager window.

Disabling and Reenabling a Static Address Mapping

When you add a NAT static address mapping, it is enabled by default. Use the BCC or Site Manager to disable or reenable it.

Using the BCC

To disable or reenable a static address mapping, navigate to the static-map prompt (for example, **box; ip; nat; domain** *<in_domain_name>***; static-map/10.1.1.1/199.1.42.200/***<out_domain_name>*) and enter:

state *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following **state disabled** command disables the static mapping entry 10.1.1.1/199.1.42.200 for a unidirectional NAT configuration:

```
nat# domain private
domain/private# static-map/10.1.1.1/199.1.42.200/public
static-map/10.1.1.1/199.1.42.200# state disabled
```

Similarly, to disable or reenable a static address mapping for bidirectional NAT, you would specify domain names other than “public” and “private.”

Using Site Manager

To disable or reenable a static address mapping, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Static Mapping**.	The NAT Static Translation List window opens.
5. Select the static mapping that you want to enable or disable from the list in the upper-left corner.	
6. Set the **Enable** parameter. Click on **Help** or see the parameter descriptions beginning on page A-13.	
7. Click on **Done**.	You return to the Configuration Manager window.

Deleting a Static Address Mapping

Use the BCC or Site Manager to delete a NAT static address mapping.

Using the BCC

To delete a static address mapping, navigate to the static-map prompt (for example, **box; ip; nat; domain** *<in_domain_name>***; static-map/10.1.1.1/199.1.42.200/***<out_domain_name>*) and enter:

delete

For example, the following **delete** command deletes the static unidirectional address mapping pair 10.1.1.1/199.1.42.200:

```
nat# domain private
domain/private# static-map/10.1.1.1/199.1.42.200/public
static-map/10.1.1.1/199.1.42.200# delete
nat#
```

Using Site Manager

To delete a static address mapping, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Static Mapping**.	The NAT Static Translation List window opens.
5. Select the static mapping that you want to delete from the list in the upper-left corner, and click on **Delete**.	The static mapping pair is deleted.
6. Click on **Done**.	You return to the Configuration Manager window.

Configuring NAT Dynamic Address Translation

For dynamic NAT to work, you must do the following:

1. **Configure NAT on the router. For instructions, see "Adding NAT to an Interface" on page 2-74.**
2. **Configure a NAT interface to each domain, whether "private," "public," or other. For instructions:**

For this type of NAT	If you want to configure using	See
Unidirectional	The BCC	"Step 6. Configure the NAT private interface" on page 2-44 and "Step 7. Configure the NAT public interface" on page 2-44
	Site Manager	"Step 1. Configure NAT on the router and specify the NAT private interface" on page 2-45 and "Step 2. Configure the NAT public interface" on page 2-46
Bidirectional	The BCC	"Step 4. Configure a NAT router interface to a device in each domain that will use NAT" on page 2-52
	Site Manager	"Steps 5, 6, 7: Configure NAT on an interface, specify a domain name, and identify a DNS server for NAT router DNS proxy" on page 2-59

3. **Configure RIP1 or RIP2 on each interface that will be used for unidirectional NAT, RIP2 on each interface that will be used for bidirectional NAT, or you can configure static routes between devices.**
   - -- For instructions on configuring RIP, see *Configuring IP, ARP, RARP, RIP, and OSPF Services.*
   - -- For instructions on configuring RIP2 using the BCC, see "Step 3. Configure RIP2 on the router IP interfaces and on each device that will use NAT" on page 2-51.
   - -- For instructions on configuring RIP2 using Site Manager, see "Step 4. Configure RIP2 on the router IP interfaces and on each device that will use NAT" on page 2-58.
4. **Configure a range of addresses as a source address filter. Instructions follow.**

5. Configure a range of addresses as a translation pool. Instructions follow.

Dynamic NAT translations are active until the specified mapping timeout value is reached. The translation remains in a translation table for as long as it is active. An idle entry is removed after a specified timeout period. If the timeout parameter is disabled, the mapping is not removed.

For instructions on how to configure mapping aging, see:

- "Enabling and Disabling the Dynamic Mapping Aging Timer" on page 2-71
- "Configuring the Dynamic Mapping Timeout Value" on page 2-72

Use the BCC or Site Manager to configure dynamic address translation. Instructions are presented in the following sections:

Topic	Page
Adding a Source Address Filter	2-97
Disabling and Reenabling a Source Address Filter	2-103
Deleting a Source Address Filter	2-105
Adding a Translation Pool	2-106
Disabling and Reenabling a Translation Pool	2-109
Deleting a Translation Pool	2-111

Adding a Source Address Filter

A *source address filter* is a range of addresses within a domain that you specify as requiring dynamic translation by the NAT router. The NAT router uses the source address filter to determine whether an IP packet requires translation for its:

- Source address (unidirectional NAT)
- Source address and destination address (bidirectional NAT)

If the packets do require translation, the source address or both the source and destination addresses are replaced by the NAT router using the next available address from a configured translation pool. (For instructions on how to configure a translation pool, see "Adding a Translation Pool" on page 2-106.)

When configuring dynamic NAT, you can create multiple source address filters and multiple translation pools for use within the same domain, provided the address ranges do not overlap. That is, the address ranges specified for one source address filter must not match another source address filter in the same domain, and the same is true of addresses between translation pools within the same domain. Overlapping address ranges are allowed between dynamic and static NAT configurations. For more information on multiple source address filters within the same domain, see "Multiple Source Address Filters -- Order of Precedence for NAT Types" on page 2-35.

Use the BCC or Site Manager to create a source address filter. Before jumping to either of these sections however, you may want to read the sections that follow. If you are configuring a source address filter for the first time, these provide general information about the parameters you set when using either of these configuration interfaces.

If you want to configure using	Go to the instructions on page
The BCC	2-100
Site Manager	2-102

IP Address and Prefix Length Parameter

To identify an address range for a source address filter, you specify the start-address parameter (in Site Manager, the IP Address parameter) and a prefix length, from 1 through 32 decimal, for a domain. The prefix length determines the number of available addresses in the source domain. For example:

If you specify this IP address	With this prefix length	Then the address range for the source router filter includes these addresses
197.0.0.0	8 (255.0.0.0)	197.0.0.0 through 197.255.255.255
197.1.2.0	24 (255.255.255.0)	197.1.2.0 through 197.1.2.255

Note: If you configure NAT on an interface with Internet Protocol Security (IPsec), make sure that the NAT source address filter subnet ranges do not overlap the IPsec filter subnet ranges.

Domain Name Parameter

When configuring a source address filter for unidirectional NAT, you must use the special domain name “private.” The reason for this is that for unidirectional NAT all hosts initiating a translation on the NAT router are from the special domain “private.” Similarly, the domain name for the translation pool for unidirectional NAT must be the opposite, “public.” Unidirectional NAT type N-to-1 requires that you configure a source address filter. (For more information, see “Configuring NAT N-to-1 Translation” on page 2-113.)

When configuring a source address filter for bidirectional NAT, you can specify any other domain name, except “private.”

Translation Pool Parameter

A router configured for dynamic NAT uses each configured source address filter in combination with a configured translation pool. To formulate this pairing, when you configure a source address filter you also identify the location of the translation pool, that is, the location of its domain in relation to the NAT router. Remembering that the NAT router is situated between two (or more) domains, you designate the translation pool as being in the domain that is either inbound to or outbound from the NAT router.

Use the BCC parameter use-translation-pool or the Site Manager parameter Translation Pool Selector to specify the translation pool location. By setting the value to *inbound*, you specify that the NAT router should use a translation pool in the same domain as the source address filter. Specifying a value of *outbound* means that you want NAT to use addresses from the translation pool in the destination domain. The default value is *outbound*. This parameter is not configurable for unidirectional NAT.

Note: If you disable or delete a translation pool or change the value of the BCC use-translation-pool parameter (in Site Manager, the Translation Pool Selector parameter) to *inbound*, the dynamic translations in the NAT mapping table do not instantly disappear. To force the removal of dynamic translation entries based on the former translation pool, modify the value of the BCC timeout-max parameter (in Site Manager, the Mapping Timeout parameter).

When configuring a source address filter for dynamic bidirectional NAT, you indicate which translation pool to use by specifying the Domain Name parameter (use the domain name associated with the source address of hosts initiating a translation on the NAT router) and the Translation Pool Selector parameter (either *inbound* or *outbound*).

For more information, see "Examples of specifying a translation pool for a source address filter" on page 2-101. Although these examples are for the BCC, the same principles apply for using Site Manager.

Static Nexthop Address Parameter

For unidirectional or bidirectional NAT, you have the option of specifying a static next hop address. Use the Static Nexthop parameter in Site Manager (next-hop-address, in the BCC) to specify statically the next hop IP address of a device with an interface to the NAT router, when this interface does not have RIP configured. The device at the static next hop address you specify makes route information available to the NAT router when handling IP traffic. If you set this parameter, then you do not have to configure RIP on the NAT interface.

Unnumbered Circuit Name Parameter

If you have any unnumbered circuits bordering your NAT router, you may need to configure the unnumbered circuit name parameter. The unnumbered circuit name parameter is optional for unidirectional NAT and is not supported for bidirectional NAT.

Using the BCC

To configure a source address filter, navigate to the domain name prompt (for example, **box; ip; nat; domain** *<name>*) and enter:

src-filter *<start_address>/<prefix_length>*

start_address specifies the start of the IP address range available for translation. Use dotted-decimal notation.

prefix_length specifies the end of the IP address range available for translation. Use an integer from 1 to 32 that represents the number of contiguous bits in the network portion.

This example for unidirectional NAT shows the creation of a domain named "private" followed by the specification of a source address filter with an address range from 10.0.0.0 to 10.255.255.255. Note that addresses 10.0.0.0 through 10.255.255.255 or address 10.0.0.0 with a prefix length of 8 is a range that is reserved for use in private networks; they are not valid on the public Internet. Use the **info** command to see the values configured for this source address filter:

```
nat# domain private
domain/private# src-filter 10.0.0.0/8
src-filter/10.0.0.0/8/private# info
   n-to-1 0.0.0.0
   next-hop-address 0.0.0.0
   prefix-length 8
   start-address 10.0.0.0
   state enabled
   type 1-to-1
   unnumbered-circuit-name {}
   use-translation-pool outbound
src-filter/10.0.0.0/8/private#
```

Because only the start-address and prefix-length parameters have been configured, the rest of the values displayed by the **info** command are default values. The values 0.0.0.0 and {} mean that these parameters have not been set, so they are inactive. The type parameter is a read-only parameter that indicates whether the type of NAT is static or dynamic (1-to-1) or N-to-1 (n-to-1).

The use-translation-pool parameter specifies that the translation pool is defined for the destination domain outbound of the NAT router. For unidirectional NAT, the value for use-translation-pool must be *outbound*. For bidirectional NAT, the value can be either *inbound* or *outbound*, the default.

Examples of specifying a translation pool for a source address filter

If you configure a source address filter for bidirectional NAT with the following address range and the outbound setting for the translation pool in domain1.net:

```
nat# domain domain1.net
domain/domain1.net# src-filter 23.4.4.4/8
src-filter/23.4.4.4/8/domain1.net# use-translation pool outbound
   use-translation-pool outbound
src-filter/23.4.4.4/8/domain1.net#
```

And you have configured this translation pool for domain1.net:

```
nat# domain domain1.net
domain/domain1.net# trans-pool 199.1.2.0/8
trans-pool/199.1.2.0/8/domain1.net#
```

Then you configure this source address filter in domain2.net:

```
nat# domain domain2.net
domain/domain2.net# src-filter 32.4.4.4/8
src-filter/32.4.4.4/8/domain2.net# use-translation pool outbound
src-filter/32.4.4.4/8/domain2.net#
```

And this translation pool for domain2.net:

```
domain/domain2.net# trans-pool 21.1.2.0/8
trans-pool/21.1.2.0/8/domain2.net#
```

If a host at 23.4.4.4 in domain1.net sends a packet into the NAT router, the router recognizes the address as belonging to the NAT source address filter and looks to the translation pool configured in the outbound domain, in this case, domain2.net. NAT dynamically assigns the next-available IP address from the translation pool, for example, 21.1.2.1, as the translated source address in the IP packet.

If you then change the source address filter in domain1.net to use translation pool *inbound*, the NAT router replaces any incoming packets whose source address matches the configured source address filter with the next available address in the translation pool defined for domain1.net, such as 199.1.2.1.

```
src-filter/23.4.4.4/8/domain1.net# use-translation pool inbound
```

Using Site Manager

To configure a source address filter, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic Mapping**.	The NAT Dynamic menu opens.
5. Choose **Source Address Filter.**	The NAT Source Address Filter List window opens.
6. Click on **Add**.	The NAT Source Address Filter Add window opens.
7. Set the following parameters, as appropriate. *For unidirectional NAT*, you must set the IP Address, Prefix Length, and Domain Name parameters (Static Nexthop and Unnumbered CCT Name are optional). Nto1 Address is specific to N-to-1 NAT. *For bidirectional NAT*, you must set the parameters required for unidirectional and also the Translation Pool Selector parameter (Static Nexthop is optional). • **IP Address** • **Prefix Length** • **Domain Name** • **Translation Pool Selector** • **Nto1 Address** • **Static Nexthop** • **Unnumbered CCT Name** Click on **Help** or see the parameter descriptions beginning on page A-28.	
8. Click on **OK**.	You return to the NAT Source Address Filter List window.

Disabling and Reenabling a Source Address Filter

When you add a source address filter, it is enabled by default. Use the BCC or Site Manager to disable or reenable it.

Using the BCC

To disable or reenable a source address filter, navigate to the src-filter prompt (for example, **box; ip; nat; domain** *<name>***; src-filter 10.1.10.0/24**) and enter:

state *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command sequence disables the source address filter 10.1.10.0/24 and verifies the change:

```
src-filter/10.1.10.0/24# state disabled
src-filter/10.1.10.0/24# info
   n-to-1 0.0.0.0
   next-hop-address 0.0.0.0
   prefix-length 24
   start-address 10.1.10.0
   state disabled
   type 1-to-1
   unnumbered-circuit-name {}
   use-translation-pool outbound
```

Using Site Manager

To disable or reenable a source address filter, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic Mapping**.	The NAT Dynamic menu opens.
5. Choose **Source Address Filter.**	The NAT Source Address Filter List window opens.
6. Select the source address filter that you want to enable or disable from the list in the upper-left corner.	The source address filter is highlighted.
7. Set the **Enable** parameter. If you place your cursor in the Enable field and click on the Values button, you can click on **Enable** or **Disable**. Click on **Help** or see the parameter description on page A-25.	
8. Click on **Done**.	Site Manager prompts you to save this change.
9. Click on **OK**.	You return to the Configuration Manager window.

Deleting a Source Address Filter

Use the BCC or Site Manager to delete a source address filter.

Using the BCC

To delete a source address filter, navigate to the source address filter prompt (for example, **box; ip; nat; domain** *<name>***; src-filter 10.1.10.0/24**) and enter:

delete

For example, the following command deletes the source address filter 10.1.10.0/24 for the domain abc.net:

```
nat# domain abc.net
domain/abc.net# src-filter 10.1.10.0/24
src-filter/10.1.10.0/24/abc.net# delete
domain/abc.net#
```

Using Site Manager

To delete a source address filter, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic Mapping**.	The NAT Dynamic menu opens.
5. Choose **Source Address Filter.**	The NAT Source Address Filter List window opens.
6. Click on the source address filter that you want to delete, and click on **Delete**.	The address range is deleted from the NAT Source Address Filter List window.
7. Click on **Done**.	You return to the Configuration Manager window.

Adding a Translation Pool

A *translation pool* is a range of IP addresses that you specify for the NAT router to use when dynamically translating the source address (in unidirectional NAT) or the source and destination addresses (in bidirectional NAT) for IP packets requiring address translation.

You can create multiple translation pools for a single domain. NAT uses the available addresses in each translation pool in sequence, starting with the lowest address. Once all the addresses in one translation pool are exhausted, NAT looks to the next pool in the same domain.

When configuring dynamic address translation, you can configure multiple translation pools and multiple source address filters for use within the same domain, although the address ranges must not overlap. That is, the address ranges specified for one translation pool must not match another translation pool in the same domain, and the same is true of addresses between source address filters within the same domain.

You specify the translation pool range of addresses as a base address and a prefix length (from 1 through 32 decimal). The prefix length determines the number of available addresses. For example:

If you specify this IP address	With this prefix length	Then the address range for the translation pool includes these addresses
197.0.0.0	8 (255.0.0.0)	197.0.0.0 through 197.255.255.255
197.1.2.0	24 (255.255.255.0)	197.1.2.0 through 197.1.2.255

Use the BCC or Site Manager to add a translation pool.

Using the BCC

To configure a translation pool, navigate to the domain name prompt (for example, **box; ip; nat; domain abc.net**) and enter:

trans-pool *<start_address>/<prefix_length>*

start_address specifies the start of the IP address range available for the translation pool. Use dotted-decimal notation.

prefix_length specifies the end of the IP address range available for translation. Use an integer from 1 to 32 that represents the number of contiguous bits in the network portion.

For example, the following command sequence configures 199.1.2.0/24 as the translation pool and verifies the entry:

```
nat# domain abc.net
domain/abc.net# trans-pool 199.1.2.0/24
trans-pool/199.1.2.0/24/abc.net# info
   prefix-length 24
   start-address 199.1.2.0
   state enabled
```

Using Site Manager

To configure a translation pool, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic Mapping**.	The NAT Dynamic menu opens.
5. Choose **Translation Pool.**	The NAT Translation Pool List window opens.
6. Click on **Add**.	The NAT Translation Pool Add window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
7. Set the following parameters: • **IP Address** • **Prefix Length** • **Domain Name** Click on **Help** or see the parameter descriptions beginning on page A-32.	
8. Click on **OK**.	You return to the NAT Translation Pool List window.
9. Click on **Done**.	You return to the Configuration Manager window.

Disabling and Reenabling a Translation Pool

When you create a translation pool, it is enabled by default. You can use the BCC or Site Manager to disable or reenable it.

Note: If you disable or delete a translation pool or change the value of the BCC use-translation-pool parameter (in Site Manager, the Translation Pool Selector parameter) to *inbound*, the dynamic translations in the NAT mapping table do not instantly disappear. To force the removal of dynamic translation entries based on the former translation pool, modify the value of the BCC timeout-max parameter (in Site Manager, the Mapping Timeout parameter).

Using the BCC

To disable or reenable a translation pool, navigate to the domain-specific translation pool prompt (for example, **box; ip; nat; domain abc.net***;* **trans-pool/199.1.2.0/24**) and enter:

state *<state>*

state is one of the following:

enabled (default)
disabled

For example, the following command sequence disables the translation pool 199.1.2.0/24 in the domain named abc.net and verifies the state:

```
trans-pool/199.1.2.0/24/abc.net# state disabled
trans-pool/199.1.2.0/24/abc.net# info
   prefix-length 24
   start-address 199.1.2.0
   state disabled
trans-pool/199.1.2.0/24/abc.net#
```

Using Site Manager

To disable or reenable a translation pool, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic Mapping**.	The NAT Dynamic menu opens.
5. Choose **Translation Pool.**	The NAT Translation Pool List window opens.
6. Select the translation pool that you want to disable or reenable from the list in the upper-left corner.	The translation pool is highlighted.
7. Set the **Enable** parameter. If you place your cursor in the Enable field and click on the Values button, you can click on **Enable** or **Disable.** Click on **Help** or see the parameter description on page A-31.	
8. Click on **Done**.	You return to the Configuration Manager window.

Deleting a Translation Pool

Use the BCC or Site Manager to delete a translation pool.

Note: If you disable or delete a translation pool or change the value of the BCC use-translation-pool parameter (in Site Manager, the Translation Pool Selector parameter) to *inbound*, the dynamic translations in the NAT mapping table do not instantly disappear. To force the removal of dynamic translation entries based on the former translation pool, modify the value of the BCC timeout-max parameter (in Site Manager, the Mapping Timeout parameter).

Using the BCC

To delete a translation pool, navigate to the domain-specific translation-pool prompt (for example, **box; ip; nat; domain abc.net trans-pool/197.1.2.0/24**) and enter:

delete

For example, the following command deletes the translation pool 197.1.2.0/24 for domain abc.net:

```
trans-pool/197.1.2.0/24/abc.net# delete
domain/abc.net#
```

Using Site Manager

To delete a translation pool, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic Mapping**.	The NAT Dynamic menu opens.
5. Choose **Translation Pool**.	The NAT Translation Pool List window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Select the translation pool that you want to delete from the list in the upper-left corner, and click on **Delete**.	The address range is deleted from the NAT Translation Pool List window.
7. Click on **Done**.	You return to the Configuration Manager window.

Configuring NAT N-to-1 Translation

NAT N-to-1 translation allows you to configure a range of addresses in a private network to be translated into a single, public IP address. N-to-1 translation has the following qualities:

- A host in the private domain initiates translation.
- Many (“N”) addresses are translated into a single address. When configuring, this single address is known as the N-to-1 address.
- Address translation is static.
- Port translation is dynamic. You do not have to configure the port translation.
- TCP and UDP are supported traffic types.
- When configuring, you must use the special domains “private” and “public.”

N-to-1 requires that RIP, RIP2, or static routes be configured on the NAT router and configured on each device in the domain “private” that will be passing traffic into the NAT router for address translation and each device in the domain “public” that receives a translated source address from the NAT router. For information on configuring RIP, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

Use the BCC or Site Manager to configure NAT N-to-1.

Using the BCC

To configure NAT N-to-1 translation, complete the following tasks:

1. **Configure a source address filter (see “Adding a Source Address Filter” on page 2-97).**
2. **Navigate to the src-filter prompt (for example, box; ip; nat; domain** *<name>***; src-filter/10.1.10.0/24) and enter:**

   n-to-1 *<IP_address>*

   IP_address is the registered IP address to be used in this N-to-1 translation. Enter this address in dotted-decimal notation.

For example, the following command sequence configures the IP address 199.1.42.100 as the address for the source address filter 10.1.10.0/24 and verifies the entry. The type parameter (read-only) reflects that this is an N-to-1 translation.

```
domain abc.net# src-filter 10.1.10.0/24
src-filter/10.1.10.0/24/abc.net# n-to-1 199.1.42.100
src-filter/10.1.10.0/24# info
   n-to-1 199.1.42.100
   next-hop-address 0.0.0.0
   prefix-length 24
   start-address 10.1.10.0
   state enabled
   type n-to-1
   unnumbered-circuit-name {}
   use-translation-pool outbound
src-filter/10.1.10.0/24#
```

Using Site Manager

To configure NAT N-to-1 translation, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic**.	The NAT Dynamic menu opens.
5. Choose **Source Address Filter.**	The NAT Source Address Filter List window opens.
6. Select a source address filter from the list in the upper-left corner, and click on **Add**.	The NAT Source Address Filter Add window opens.
7. Set the following parameters: • **IP Address** • **Prefix Length** • **Domain Name** • **Nto1 Address** Click on **Help** or see the parameter descriptions beginning on page A-28.	
8. Click on **Done**.	You return to the Configuration Manager window.

Chapter 3
Configuring RIPSO on an IP Interface

This chapter describes RIPSO and provides instructions for configuring RIPSO on an IP interface.

Topic	Page
RIPSO Concepts and Terminology	3-2
Enabling and Disabling RIPSO	3-6
Specifying the IP Datagram Type for Stripping Security Options	3-7
Specifying the Outbound Datagram Type Requiring Security Labels	3-8
Specifying the Inbound Datagram Type Requiring Security Labels	3-9
Setting the Security Level for IP Datagrams	3-10
Choosing Authority Flags in Outbound Datagrams	3-11
Choosing Authority Flags in Inbound Datagrams	3-12
Supplying Implicit Labels for Unlabeled Inbound Datagrams	3-13
Enabling and Disabling Default Labels for Unlabeled Outbound Datagrams	3-14
Enabling and Disabling Error Labels for Outbound ICMP Error Datagrams	3-15
RIPSO Example	3-16

RIPSO Concepts and Terminology

IP routers support the Department of Defense (DoD) Revised IP Security Option (RIPSO), as defined in RFC 1108, on a per-interface basis. RFC 1108 specifies both “basic” and “extended” security options; the Nortel Networks implementation supports only the basic option.

RIPSO allows end systems and intermediate systems (routers) to add labels to or process security labels in IP datagrams that they transmit or receive on an IP network. The labels specify security classifications (for example, Top Secret, Secret, Confidential, and Unclassified, in descending order), which can limit the devices that can access these labeled IP datagrams.

As a labeled IP datagram traverses an IP network, only those systems that have the proper clearance (that is, whose security classification range covers the classification specified by the datagram) should accept and forward the datagram.

Any system whose security classification range does not cover the classification specified by the security label should drop the datagram.

Note: RIPSO does not include any method of preventing a system that does not support RIPSO from simply accepting and forwarding labeled datagrams. Thus, in order for RIPSO to be effective, *all* systems in a network must support RIPSO and process IP datagrams as described.

By default, RIPSO is disabled on IP interfaces. You can use Site Manager to enable RIPSO on an IP interface and specify the following:

- A range of acceptable security levels for IP datagrams that the interface receives and transmits
- A set of required and allowed authority values for IP datagrams that the interface receives and transmits
- Whether inbound datagrams received on this interface require security labels
- Whether outbound datagrams transmitted on this interface (either forwarded or originated by the router) require security labels
- Whether datagrams received or transmitted on this interface should have their labels stripped

You also specify whether the router creates the following types of labels:

- An implicit label, which the router uses to label unlabeled inbound datagrams, when required
- A default label, which the router uses to label unlabeled outbound datagrams, when required
- An error label, which the router uses to label Internet Control Message Protocol (ICMP) error messages associated with processing security options

Security Label Format

A RIPSO security label is three or more bytes long and specifies the security classification level and protection authority values for the datagram (Figure 3-1).

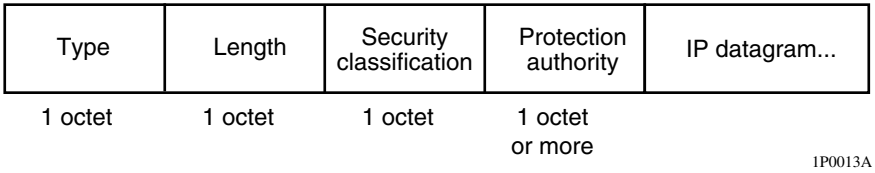


Figure 3-1. RIPSO Security Label

The format of the security label is as follows:

- Octet 1 contains a type value of $82_{(16)}$, identifying the basic security option format.
- Octet 2 specifies the length of the option (three or more octets, depending on the presence or absence of authority flags).
- Octet 3 specifies the security classification levels for the datagrams. Valid security classification levels include:

$3D_{(16)}$	Top Secret
$5A_{(16)}$	Secret
$96_{(16)}$	Confidential
$AB_{(16)}$	Unclassified

- Octet 4 and beyond identify the protection authorities under whose rules the datagram is classified at the specified level. (If no authorities have been identified, then this field is not used.)

  The first 7 bits (0 through 6) are flags. Each flag represents a protection authority. The flags defined for octet 4 are as follows:

Bit 0	GENSER	General Services (as per DoD 5200.28)
Bit 1	SIOP-ESI	DoD (Organization of the Joint Chiefs of Staff)
Bit 2	SCI	Central Intelligence Agency
Bit 3	NSA	National Security Agency
Bit 4	DOE	Department of Energy
Bit 5	Reserved	
Bit 6	Reserved	
Bit 7	Termination indicator	

Note: Bit 7 acts as a “more” bit, indicating that another octet (containing additional authority flags) follows.

Inbound IP Datagrams

When the router receives an IP datagram on a RIPSO interface, it compares the security classification and authority values specified in the security label with those configured on the inbound interface.

If the interface does *not* require a security label for inbound IP datagrams, the router accepts both unlabeled IP datagrams and datagrams that meet the classification and authority rules described in the next paragraph.

If the interface *does* require a security label, then for the router to accept the datagram, the following RISPO conditions must be met:

- The datagram must be labeled.
- The security classification value in the datagram’s label must be within the security-level range configured for the interface.

- The authority flags in the datagram's label must include all flags required for the interface and cannot contain any flags not allowed for the interface.

The router drops any datagrams that do not meet these requirements and generates an ICMP error message.

On a non-RIPSO interface, the router accepts only unlabeled IP datagrams and IP datagrams that are labeled as Unclassified with no authority flags set.

Forwarded IP Datagrams

When the router receives an IP datagram that needs forwarding on a RIPSO interface, the router compares the security classifications and authority values specified in the security label with those configured on the outbound interface. Before forwarding the datagram, the router:

- Checks that all RIPSO conditions are met (see the preceding section)
- Applies any outbound-specific configuration parameters

The router drops any datagrams that do not meet these requirements and generates an ICMP error message.

Originated IP Datagrams

When the router originates a datagram and the following conditions are true, the router labels the datagram with the default security label before transmitting it:

- The datagram needs forwarding through a RIPSO interface.
- The RIPSO interface requires outbound labels for originated datagrams.

Unlabeled IP Datagrams

If the router receives an unlabeled IP datagram from an interface on which RIPSO is *not* enabled (or on which labels are not required for inbound datagrams), and the IP datagram needs forwarding to an interface on which RIPSO *is* enabled and labels are required for outbound datagrams, then the router labels the datagram, using either an implicit label or a default label as follows:

- If the inbound interface has an implicit label configured, the router uses it to label the datagram.

- If the inbound interface does not have an implicit label configured, the router labels the datagram with the default label configured for the outbound interface.

If the interface does not have an implicit or default label configured, the datagram is dropped.

Enabling and Disabling RIPSO

Use Site Manager to enable or disable RIPSO on an interface. When you disable RIPSO, the router accepts only the following IP datagrams: labeled IP datagrams with the classification level set to Unclassified and no authority flags set, and unlabeled IP datagrams.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Click on the interface that you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Enable Security** parameter. Click on **Help** or see the parameter description on page A-35.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying the IP Datagram Type for Stripping Security Options

Use Site Manager to choose the type of IP datagram from which you want IP security options to be removed. Options are:

- None. The router leaves IP security options on all inbound and outbound IP datagrams intact.
- Incoming. The router strips the IP security option from each incoming IP datagram after checking the IP datagram against the interface's security configuration.
- Outgoing. The router strips the IP security option from each outgoing IP datagram before checking each datagram against the interface's security configuration.
- All. The router strips the IP security options from both incoming and outgoing IP datagrams: incoming datagrams after checking each against this interface's security configuration, and outgoing datagrams before checking each against the interface's security configuration.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Click on the interface that you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Strip Security** parameter. Click on **Help** or see the parameter description on page A-35.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying the Outbound Datagram Type Requiring Security Labels

Use Site Manager to specify the type of outbound datagrams that require IP security labels. Options are:

- None. The router forwards unlabeled IP datagrams unchanged on this interface. In addition, those IP datagrams that it originates and transmits do not require labels.
- Forwarded. All IP datagrams that the router forwards on this interface (not those it originates) must contain basic IP security options. If the datagram already contains an IP security label, the router forwards the datagram unchanged. If the datagram is unlabeled, the router adds the implicit or default label to the datagram before forwarding it.
- Originated. The router specifies basic IP security options for all IP datagrams that it originates and transmits on this interface. The router adds the default label to IP datagrams that it originates and transmits on this interface.
- All. All datagrams (both those that the router forwards and those it originates) on this interface must contain basic IP security options. RIPSO supplies the implicit or default label for those datagrams that do not already contain one.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Click on the interface that you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Require Out Security** parameter. Click on **Help** or see the parameter description on page A-36.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Specifying the Inbound Datagram Type Requiring Security Labels

Use Site Manager to specify the type of inbound datagrams that require IP security labels. Options are:

- None. Inbound IP datagrams are not required to contain labels.
- All. All inbound IP datagrams received on this interface must contain basic IP security options.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Click on the interface that you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Require In Security** parameter. Click on **Help** or see the parameter description on page A-36.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Setting the Security Level for IP Datagrams

Use Site Manager to specify the minimum and maximum security level that the router allows for inbound or outbound IP datagrams. The minimum and maximum security level features specify the range of classification levels that the router will accept and process. The router drops IP datagrams received on this interface that are below the minimum and above the maximum levels that you specify.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Click on the interface that you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the following parameters: • **Minimum Level** • **Maximum Level** Click on **Help** or see the parameter descriptions beginning on page A-37.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Choosing Authority Flags in Outbound Datagrams

Use Site Manager to specify which authority flags *must* be set, and which authority flags *may* be set in the protection authority field of all outbound datagrams.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Click on the interface that you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the following parameters: • **Must Out Authority** • **May Out Authority** Click on **Help** or see the parameter descriptions beginning on page A-38.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Choosing Authority Flags in Inbound Datagrams

Use Site Manager to specify which authority flags *must* be set, and which authority flags *may* be set in the protection authority field of all inbound datagrams.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Click on the interface that you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the following parameters: • **Must In Authority** • **May In Authority** Click on **Help** or see the parameter descriptions beginning on page A-39.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Supplying Implicit Labels for Unlabeled Inbound Datagrams

Use Site Manager to specify whether the router should supply implicit labels to unlabeled inbound datagrams received by an interface. The router uses the values of the Implicit Authority and Implicit Level parameters to create an implicit label. By default, implicit labeling is enabled.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Click on the interface that you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the following parameters: • **Implicit Label** • **Implicit Authority** • **Implicit Level** Click on **Help** or see the parameter descriptions beginning on page A-40.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Enabling and Disabling Default Labels for Unlabeled Outbound Datagrams

Use Site Manager to specify whether you want the router to supply a default label to unlabeled outbound datagrams originated or forwarded out this interface. The router uses the values of the Default Authority and Default Level parameters to create a default label.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Click on the interface that you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the following parameters: • **Default Label** • **Default Authority** • **Default Level** Click on **Help** or see the parameter descriptions beginning on page A-41.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

Enabling and Disabling Error Labels for Outbound ICMP Error Datagrams

Use Site Manager to specify whether you want the router to supply an error label to outbound ICMP error datagrams. The router uses the values of the Error Authority and the Minimum Level parameters to create an error label.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Click on the interface that you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the following parameters: • **Error Label** • **Error Authority** Click on **Help** or see the parameter descriptions beginning on page A-43.	
6. Click on **Apply**, and then click on **Done**.	You return to the Configuration Manager window.

RIPSO Example

The router in Figure 3-2 has RIPSO configured on all three IP interfaces. The security ranges specified for each interface vary, as shown. (For simplicity, this example assumes that none of the interfaces requires any authority flags on inbound and outbound traffic, but any flags that are present are acceptable.)

When host 1.1.0.1 broadcasts an all-subnets broadcast IP datagram with the security-level classification set to Secret, the router compares the datagram's classification with the range configured on inbound interface 1.1.0.2. Because the Secret security level is within the range configured on the interface, the router accepts the datagram. In order to forward the datagram, the router does the following:

- Compares the datagram's security level, Secret, to the security-level ranges configured on interfaces 1.2.0.2 and 1.3.0.2
- Forwards the datagram on interface 1.2.0.2, because Secret is within the security range configured on the interface
- Does *not* forward the datagram on interface 1.3.0.2, because Secret is outside the security range configured on the interface

Interface	Min. Security Classification	Max. Security Classification
1.1.0.2	Unclassified	Top secret
1.2.0.2	Secret	Top secret
1.3.0.2	Top secret	Top secret

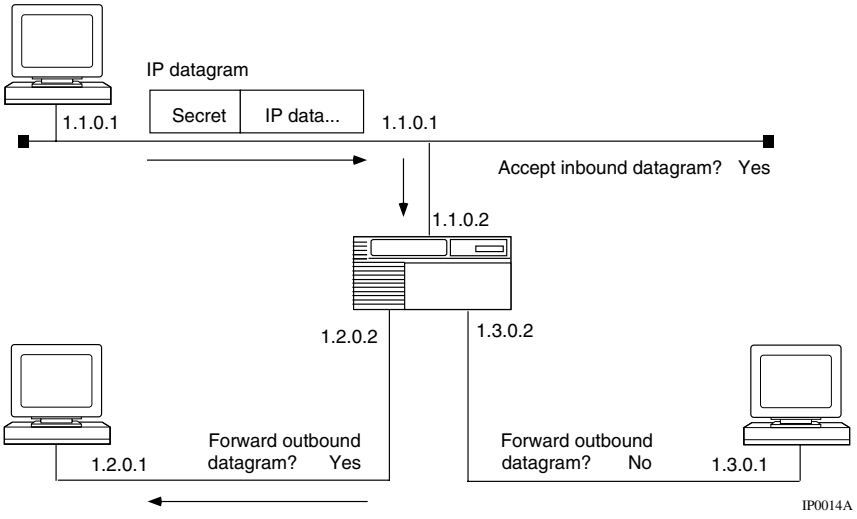


Figure 3-2. RIPSO Example

Chapter 4
Connecting the Router to a Blacker Front End

This chapter describes the Blacker front end (BFE) and provides instructions for configuring the BFE on a router.

Topic	Page
Blacker Front End (BFE) Concepts and Terminology	4-2
BFE Addressing	4-4
Configuring BFE Support	4-5

Blacker Front End (BFE) Concepts and Terminology

The BFE is a classified encryption device used by hosts to communicate across unsecured wide area networks (WANs). BFE devices are typically found in government networks (for example, DSNET), which handle sensitive data requiring a greater degree of security.

BFE support allows the router to connect to BFE devices. The BFE device, in turn, provides the router with encryption services while acting as the data communication equipment (DCE) end of the connection between the router and the X.25 network.

Hosts using attached BFE devices can communicate with each other over an unsecured packet-switched network using data paths secured by the encryption services of the BFE devices.

BFE devices provide encryption services for connections over the unsecured portions of packet-switched networks (Figure 4-1). Hosts with BFEs are part of a *red* virtual network. The packet-switched network that carries both the data secured by BFE devices and any other unsecured data is known as the *black* network.

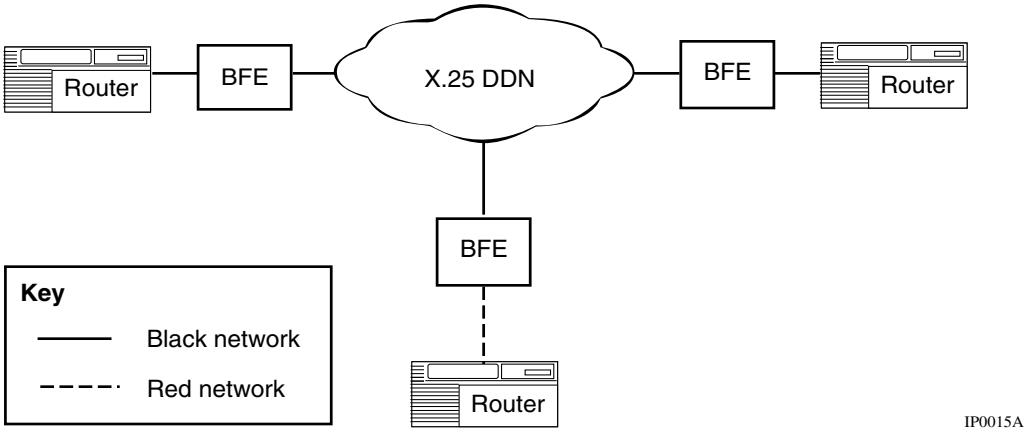


Figure 4-1. BFE Network Configuration

BFE devices receive authorization and address translation services from an access control center (ACC) residing on the black network. The ACC makes access control decisions that determine which hosts are allowed to communicate with each other. A key distribution center (KDC) residing on the black network provides encryption keys and key management services. A BFE device uses these encryption keys for encrypting traffic between itself and other BFE devices.

The router-to-BFE interface is a modified version of the interface presented in the 1983 DDN X.25 Host Interface Specification. It supports data rates between 1200 b/s and 64 KB/s. To support BFE services, Revised IP Security Option (RIPSO) must be enabled on the IP interface. All IP datagrams transmitted on the interface must contain a RIPSO security label. The first option in each IP datagram header must be the Basic Security option.

BFE Addressing

You can enable BFE support on individual IP interfaces. Once enabled, the router uses the BFE address-resolution algorithm to map IP addresses to corresponding X.121 addresses.

BFE IP-to-X.121 address translation differs from standard DDN address translation. Each physical router-to-BFE connection is identified by a BFE X.121 network address and a BFE IP address. The format of a BFE X.121 address is:

zzzzzpdddbbb

zzzzz	is 0
p	is the BCD encoding of the port ID
ddd	is the BCD encoding of the domain ID
bbb	is the BCD encoding of the BFE ID

All BFE hosts are members of Class A IP networks. The format of a BFE IP address is as follows:

nnnnnnnn.Zpppdddd.dddddbb.bbbbbbbb

nnnnnnnn	identifies the network ID in bits
Z	is 0
ppp	is the port ID in bits
dddd.dddddd	is the domain ID in bits
bb.bbbbbbbb	is the BFE ID in bits

BFE supports only physical addressing. It does not support logical addresses or subaddresses.

Configuring BFE Support

To configure BFE support on an IP interface, you must:

- Configure an X.25 interface that conforms to the BFE requirements described in this section.
- Enable the IP routing protocol on the interface.
- Enable RIPSO support on the interface.

Beginning at the Configuration Manager window, perform the following procedures:

1. **Configure an X.25 interface.**

   When you initially configure packet-level parameters for the X.25 interface, make certain to:

   a. **Set the Network Address Type parameter to BFE_NETWORK.**

   b. **Set the DDN IP Address parameter to the IP address that is assigned to your BFE connection.**

2. **Edit the packet-layer parameters for the X.25 interface to match the settings specified in Table 4-1.**
3. **Add network service records to the X.25 interface.**
4. **Edit the network service record parameters for the X.25 interface to match the settings specified in Table 4-2.**

   Remember to set the DDN BFE parameter to Enable.

5. **Enable the IP routing protocol on the X.25 interface.**

   The specified IP address must match the one specified in the packet-layer parameter setting.

6. **Edit the IP interface record.**

   The address resolution must be set to X.25 BFE DDN. Also, configure IP security options (RIPSO) on the interface. IP security must be enabled, and labels are required on all outbound data.

For instructions on performing steps 1 through 4, see *Configuring X.25 Services*. For instructions on performing step 5, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*. For instructions on performing step 6, see Chapter 3, "Configuring RIPSO on an IP Interface."

Note: Generally, the synchronous line parameter settings are the same for both a DDN X.25 link and a BFE X.25 link. However, if your operating environment has specific needs, you may want to edit synchronous line parameters. For instructions, see *Configuring WAN Line Services*.

Table 4-1. BFE X.25 Packet-Level Parameter Settings

Parameter	Setting
Enable	Enable
Network Address Type	BFE_NETWORK
PDN X.121 Address	Parameter is ignored.
DDN IP Address	Specify the IP address assigned to your BFE connection.
Sequence Size	MOD8
Restart Procedure Type	DTE_RESTART
Default Tx/Rx Window Size	Range is 2 to 7. This setting should match the default value configured in the BFE. This value should be coordinated with the X.25 service record value.
Default Tx/Rx Packet Length	Options include 128, 256, 512, and 1024. This setting should match the default value configured in the BFE. This value should be coordinated with the X.25 service record value.
Number of incoming SVC channels	Zero (0). BFE does not support the one-way logical channel incoming facility.
Incoming SVC LCN Start	Parameter is ignored.
Number of outgoing SVC channels	Any valid nonzero setting.
Bidirectional SVC LCN	Any valid nonzero setting.
Number of outgoing SVC channels	Zero (0). BFE does not support the one-way logical channel outgoing facility.

(continued)

Table 4-1. BFE X.25 Packet-Level Parameter Settings *(continued)*

Parameter	Setting
Outgoing SVC LCN Start	Parameter is ignored.
Number of PVC channels	Zero (0). BFE does not support PVCs.
PVC LCN Start	Parameter is ignored.
T1 Timer, T2 Timer, T3 Timer, T4 Timer	BFE has no special requirements for any of these four parameters.
Flow Control Negotiation	Set to on if you do not want to use the default values configured in the BFE for this link.
Max Window Size	Range is 2 to 7. If you specify any setting other than the default value configured in the BFE, set Flow Control Negotiation to on. This value should be coordinated with the X.25 service record value.
Max Packet Length	Options include 128, 256, 512, and 1024. If you specify any value other than the default value configured in the BFE, then set Flow Control Negotiation to on. (If the IP interface is configured to support multiple IP security levels, then set to 1024.) This value should be coordinated with the X.25 service record value.
Trans/Recv Throughput Class	Parameter is ignored.
Max Throughput Class	Parameter is ignored.
Throughput Class Negotiation	Off
Network User Identification	Off
Incoming Calls Accept	On
Outgoing Calls Accept	On
Fast Select Accept	Off
Reverse Charge Accept	Off
Fast Select	Off
Reverse Charging	Off
CUG Selection	Null
CUG Outgoing Access	Null
CUG Bilateral Selection	Null
RPOA Selection	Off
Charging Information	Off
Transit Delay	Off

(continued)

Table 4-1. BFE X.25 Packet-Level Parameter Settings *(continued)*

Parameter	Setting
Full Addressing	On
Acceptance Format	Defext
Release Format	Defext
CCITT (now ITU-T) Conformance	DXE1980
Network Standard	DOD

Table 4-2. BFE X.25 Network Service Record Parameter Settings

Parameter	Setting
Enable	Enable
Type	DDN
Connection ID	Parameter is ignored.
Remote IP Address	Specify the IP address of the remote system.
Remote X.121 Address	Parameter is ignored.
Broadcast	Parameter is ignored.
Max Connections	Any valid setting
Precedence	Any valid setting. The BFE will accept, but not act on, the DDN Precedence facility.
Max Idle	Any valid setting
Call Retry	Any valid setting
Flow Facility	Set to on if you want to use a value other than the default window size and packet size configured in the BFE.
Window Size	Range is 2 to 7. If you want to use a value other than the default window size configured in the BFE, set Flow Facility to on. You must coordinate this value with the packet-level value.

(continued)

Table 4-2. BFE X.25 Network Service Record Parameter Settings *(continued)*

Parameter	Setting
Packet Size	Options include 128, 256, 512, and 1024. If you want to use a value other than the default packet size configured in the BFE, set Flow Facility to on. (If the IP interface is configured to support multiple IP security levels, then set to 1024.) You must coordinate this value with the packet-level value.
Fast Select Request	Off
Fast Select Accept	Off
Reverse Charge Request	Off
Reverse Charge Accept	Off
User Facility	Null
DDN BFE	Enable
CUG Facility Format	None
CUG Facility Type	Parameter is ignored.
CUG Number	Parameter is ignored.

Appendix A
Site Manager Parameters

This appendix contains the Site Manager parameter descriptions for GRE, NAT, and RIPSO. You can display the same information using Site Manager online Help.

This appendix contains the following information:

Topic	Page
GRE Parameters	A-2
NAT Parameters	A-7
RIPSO Parameters	A-34

For each parameter, this appendix provides the following information:

- Parameter name
- Configuration Manager menu path
- Default setting
- Valid parameter options
- Parameter function
- Instructions for setting the parameter
- Management information base (MIB) object ID

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, see *Using Technician Interface Software*.

Caution: The Technician Interface does not verify the validity of your parameter values. Entering an invalid value can corrupt your configuration.

GRE Parameters

This section lists and describes GRE tunnel parameters.

GRE Tunnel Parameters

The GRE Create Tunnels List window (Figure A-1) allows access to parameters that configure a GRE tunnel.

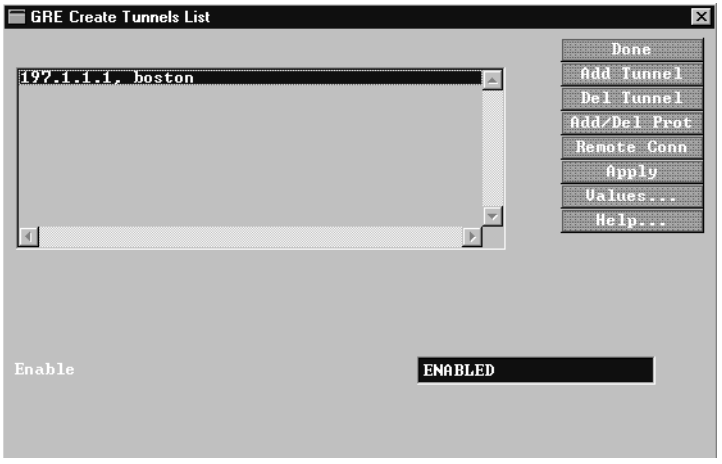


Figure A-1. GRE Create Tunnels List Window

To access the GRE Create Tunnels List window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.

Parameter: Tunnel Name

Path: Configuration Manager > Protocols > IP > GRE > Add Tunnel
Default: None
Options: Any name up to 32 characters
Function: Identifies the GRE tunnel.
Instructions: Enter a name.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.27.1.5

Parameter: IP Interface

Path: Configuration Manager > Protocols > IP > GRE > Add Tunnel
Default: None
Options: IP interface address
Function: Specifies the IP address of the physical router interface at the local end of the GRE tunnel. This address is visible to the network cloud that the tunnel passes through.
Instructions: Enter the IP address of the appropriate local IP interface in dotted-decimal notation.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.27.1.7

Parameter:	**Enable**
Path:	Configuration Manager > Protocols > IP > GRE
Default:	Enabled
Options:	Enabled | Disabled
Function:	Enables or disables the tunnel.
Instructions:	Set to Enable to enable the tunnel. Set to Disable to disable the tunnel.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.27.1.2

Remote Connection Parameters

The Create GRE Remote Connection window (Figure A-2) allows access to parameters that configure remote tunnel end points.

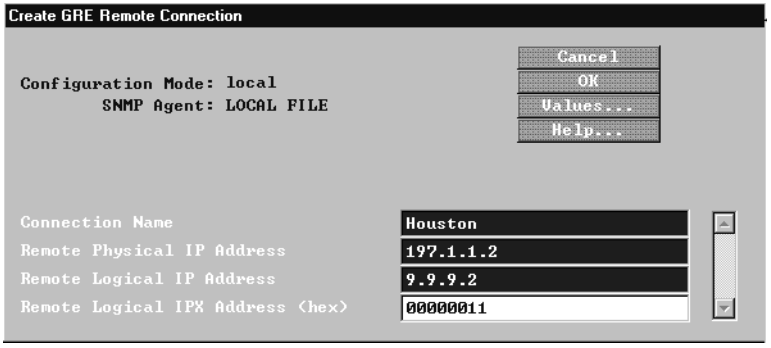


Figure A-2. Create GRE Remote Connection Window

To access the Create GRE Remote Connection window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **GRE**.	The GRE Create Tunnels List window opens.
4. Choose a tunnel from the list and click on **Remote Conn**.	The GRE Remote Connections List window opens.
5. Click on **Add**.	The Create GRE Remote Connection window opens.

Parameter: Connection Name

Path: Configuration Manager > Protocols > IP > GRE > Remote Conn
Default: Null
Options: Any name up to 32 characters
Function: Identifies the remote tunnel end point.
Instructions: Enter the appropriate connection name.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.28.1.5

Parameter: Enable

Path: Configuration Manager > Protocols > IP > GRE > Remote Conn
Default: Enable
Options: Enable | Disable
Function: Enables or disables the remote connection.
Instructions: Set to Enable to enable the remote connection. Set to Disable to disable the remote connection.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.28.1.2

Parameter: Remote Physical IP Address

Path: Configuration Manager > Protocols > IP > GRE > Remote Conn
Default: 0.0.0.0
Options: IP interface address
Function: Specifies the IP address of the physical router interface at the remote end of the GRE tunnel. This address is visible to the network cloud that the tunnel passes through.
Instructions: Enter an IP address in dotted-decimal notation.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.28.1.6

Parameter: Remote Logical IP Address

Path: Configuration Manager > Protocols > IP > GRE > Remote Conn > Add
Default: None
Options: IP interface address
Function: Specifies the address of the IP interface configured at the remote end of the GRE tunnel. This address is not visible to the network cloud that the tunnel passes through.
Instructions: Enter the appropriate IP address in dotted-decimal notation.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.6.1.1

Parameter: Remote Logical IPX Address (hex)

Path: Configuration Manager > Protocols > IP > GRE > Remote Conn > Add
Default: None
Options: Valid IPX address of the remote host
Function: Specifies the address of the IPX interface configured at the remote end of the GRE tunnel. This address is not visible to the network cloud that the tunnel passes through.
Instructions: Enter an IPX address up to 12 hexadecimal characters.
MIB Object ID: 1.3.6.1.4.1.18.3.5.5.26.1.5

NAT Parameters

NAT parameters are described in the following sections:

Topic	Page
NAT Global Parameters	A-7
NAT Interface Parameters	A-11
NAT Static Translation Parameters	A-12
NAT Dynamic Mapping Parameters	A-24

NAT Global Parameters

The NAT Global Configuration window allows access to NAT global configuration parameters. Before you can start NAT on the router, you must configure a circuit that the protocol can use as an interface to an attached network. For instructions, see *Configuring Ethernet, FDDI, and Token Ring Services* or *Configuring WAN Line Services*.

If IP has already been configured for the circuit, complete the following tasks to access the NAT Global Configuration window.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the connector that you want to configure as the NAT private interface.	The Edit Connector window opens.
2. Click on **Edit Circuit**.	The Circuit Definition window opens.
3. Choose **Protocols**.	The Protocols menu opens.
4. Choose **Add/Delete**.	The Select Protocols window opens, with a check mark next to IP.
5. Click on **NAT**.	A check mark appears next to NAT.
6. Click on **OK.**	The NAT Global Configuration window opens.

Parameter:	**Enable**
Path:	Configuration Manager > Protocols > IP > NAT > Global
Default:	Enable
Options:	Enable | Disable
Function:	Enables or disables NAT on the router. If enabled, NAT performs network address translation. If disabled, no network translation occurs.
Instructions:	To enable NAT on the entire router, set to Enable. To disable NAT, set to Disable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.7.1.2

Caution: Any interface used to forward packets translated by NAT must be configured as a NAT global interface. Otherwise, packets may be dropped.

Parameter:	**Soloist Slot Mask**
Path:	Configuration Manager > Protocols > IP > NAT > Global
Default:	A bit mask value that means all slots except for slot 1.
Options:	One or more slot numbers
Function:	Specifies the slots on which NAT can run as a soloist.
Instructions:	Set the bits on the soloist slot mask by entering a 1 in the correct bit position in the mask. The leftmost bit represents the slot with the lowest number. For example, if a router has five slots, you can configure a slot mask to allow NAT to run as a soloist on slots 3 and 5 by entering the binary value 00101.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.7.1.4

Parameter: Log Mask

Path: Configuration Manager > Protocols > IP > NAT > Global

Default: 0x00000000 (meaning that no message type is specified)

Options: One or more log mask types

Function: Specifies the types of log messages that are reported by NAT software.

Instructions: Click on Values and select the message type that you want to log. You can choose to log messages for one or more of the following types: MIB, IP, forwarding, mapping, or aging.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.1.6

Parameter: Mapping Aging

Path: Configuration Manager > Protocols > IP > NAT > Global

Default: Enable

Options: Enable | Disable

Function: Enables or disables mapping aging for a dynamic NAT entry. If there are no translated packets for a specific address mapping within the time period specified by the Mapping Timeout (secs) parameter, NAT software removes the entry from the dynamic mapping entry list, freeing the address for another mapping.

Instructions: To enable the translation entry mapping aging feature on the router, set to Enable. To disable this feature, set to Disable. This parameter is not applicable for NAT static mapping entries.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.1.7

Parameter: Mapping Timeout (secs)

Path: Configuration Manager > Protocols > IP > NAT > Global

Default: 3600 seconds (equivalent to 1 hour)

Options: 1 to 2,147,483,647 seconds

Function: Specifies, in seconds, the mapping timeout period for a dynamic NAT entry. If there are no translated packets for a specific address mapping within this time period, NAT software removes the entry from the dynamic mapping entry list, freeing the address for another mapping.

Instructions: Specify the timeout period. The maximum value, 2,147,483,647 seconds, is equivalent to approximately 68 years.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.1.8

Parameter: Install Private Address

Path: Configuration Manager > Protocols > IP > NAT > Global

Default: Enable

Options: Enable | Disable

Function: Specifies whether unidirectional NAT is backward compatible with versions before BayRS 14.20. If enabled, NAT will install in the routing table of the NAT router any private addresses learned from interfaces configured for unidirectional NAT.

Instructions: To preserve unidirectional private address translations (whether static or dynamic) configured before BayRS 14.20, set this parameter to Enable. To specify that such private addresses should not appear in the routing table, set to Disable. This parameter is ignored for bidirectional NAT.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.1.18

NAT Interface Parameters

The NAT Interface List window allows access to NAT interface parameters. If you have already configured NAT globally on a router, complete the following tasks to access the NAT Interface List window:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Interface**.	The NAT Interface List window opens.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > NAT > Interface

Default: Enable

Options: Enable | Disable

Function: Enables or disables NAT on an IP interface.

Instructions: To enable NAT on an IP interface, set to Enable. To disable NAT on an IP interface, set to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.11.1.2

Parameter: Domain Name

Path: Configuration Manager > Protocols > IP > NAT > Interface

Default: Private

Options: For unidirectional NAT: Public or Private
For bidirectional NAT: any valid domain name except Public or Private

Function: Specifies the domain to which this interface is connected.

Instructions: For unidirectional NAT, set this parameter to either Public or Private. For bidirectional NAT, specify a domain name for a network that is connected to this NAT router interface.

A domain name is a sequence of labels separated by periods. A label can contain up to 63 characters. A label must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or a hyphen. For example, my-company3.com is an acceptable domain name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.11.1.5

NAT Static Translation Parameters

The NAT Static Translation List window allows access to NAT static mapping parameters. To access the NAT Static Translation List window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Static Mapping**.	The NAT Static Translation List window opens.

Parameter: Enable

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping
Default: Enable
Options: Enable | Disable
Function: Enables or disables a static address translation.
Instructions: To enable a static address translation (mapping pair entry in NAT translation table), set to Enable. To disable a static address translation, set to Disable.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.2

Parameter: Private Address

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping
Default: None
Options: Any IP address
Function: Specifies the original address of the host in the source domain for this static translation. Within a static mapping pair of addresses, this is the untranslated address.
Instructions: Enter the appropriate IP address in dotted-decimal notation.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.3

Parameter: Private Port

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping
Default: 0
Options: None
Function: Specifies the original UDP or TCP port for this static translation. (Within a static mapping pair of ports, this is the untranslated port.)
Instructions: Enter the domain-specific port number.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.6

Parameter:	**Source Domain**
Path:	Configuration Manager > Protocols > IP > NAT > Static Mapping
Default:	For unidirectional NAT: Private For bidirectional NAT: no default
Options:	For unidirectional NAT: Private For bidirectional NAT: any valid domain name for a network connected to a NAT router interface
Function:	Specifies the name of the inbound domain for this static unidirectional or SDPT translation. This translation will be valid only for packets with IP source addresses coming inbound to the NAT router from this domain.
Instructions:	For static translation types unidirectional or SDPT, accept the default domain name, Private. Otherwise, specify a domain name for a network that is connected to a NAT router interface. A domain name is a sequence of labels separated by periods. A label can contain up to 63 characters. A label must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or a hyphen. For example, my-company3.com is an acceptable domain name.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.7.9.1.8

Parameter: Destination Domain

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping

Default: For unidirectional NAT: Public
For bidirectional NAT: no default

Options: For unidirectional NAT: Public
For bidirectional NAT: any valid domain name for a network connected to a NAT router interface

Function: Specifies the name of the outbound domain for this static unidirectional or SDPT translation. This translation is valid only for packets that are forwarded out from the NAT router into this domain.

Instructions: For NAT static translation types unidirectional or SDPT, accept the default domain name, Public. Otherwise, specify a domain name for a network that is connected to a NAT router interface.

A domain name is a sequence of labels separated by periods. A label can contain up to 63 characters. A label must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or a hyphen. For example, my-company3.com is an acceptable domain name.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.9

Parameter: Static Nexthop

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping

Default: 0.0.0.0

Options: Any IP address

Function: Specifies the IP address of the next hop for this static translation.

Instructions: Enter the IP address of an interface that is directly connected to the NAT router. This address must be in the same subnet as the Source Domain. A value of 0.0.0.0 means that there is no Static Nexthop address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.10

Parameter: Unnumbered CCT Name

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping

Default: None

Options: Any unnumbered circuit name

Function: Specifies that this static unidirectional translation will occur over this unnumbered interface.

Instructions: If you have not configured any unnumbered interfaces, leave this parameter blank. Otherwise, specify the appropriate circuit name from the list of configured unnumbered circuits. To view a list of the available unnumbered circuits, click on Values. The Unnumbered CCT Name parameter is supported for unidirectional NAT only.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.11

Adding Static Translation Parameters

To add static translations, whether bidirectional, SDPT, or unidirectional, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Static Mapping**.	The Static Mapping menu opens.
5. Click on **Add.**	The Add Translation Type window opens.
6. Choose from **Bidirectional, SDPT**, or **Unidirectional**.	The appropriate window opens.

Depending on the type of configuration you want, go to the appropriate section:

Topic	Page
Adding NAT Bidirectional Parameters	A-17
Adding NAT SDPT Parameters	A-20
Adding NAT Unidirectional Parameters	A-22

Adding NAT Bidirectional Parameters

To configure NAT static bidirectional port translation, configure the following parameters:

Parameter: Private Address

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > Bidirectional

Default: None

Options: IP address

Function: Specifies the original address of the host in the source domain for this static translation. Within a NAT static mapping pair of addresses, this is the untranslated address.

Instructions: Enter the appropriate IP address in dotted-decimal notation.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.3

Parameter:	**Source Domain**
Path:	Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > Bidirectional
Default:	For unidirectional NAT: Private For bidirectional NAT: no default
Options:	For unidirectional NAT: Private For bidirectional NAT: any valid domain name for a network connected to a NAT router interface.
Function:	Specifies the name of the inbound domain for this static unidirectional or SDPT translation. This translation is valid only for source addresses coming inbound to the NAT router from this domain.
Instructions:	For static translation types unidirectional or SDPT, accept the default domain name, Private. Otherwise, specify a domain name for a network that is connected to a NAT router interface. The domain name must be in accordance with RFC 1035.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.7.9.1.8

Parameter:	**Public Address**
Path:	Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > Bidirectional
Default:	None
Options:	IP address
Function:	Specifies the public or external address for this static translation.
Instructions:	Enter the appropriate IP address in dotted-decimal notation.
MIB Object ID:	Not available.

Parameter: Destination Domain

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > Bidirectional

Default: For unidirectional NAT: Public
For bidirectional NAT: no default

Options: For unidirectional NAT: Public
For bidirectional NAT: any valid domain name for a network connected to a NAT router interface

Function: Specifies the name of the outbound domain for this static unidirectional or SDPT translation. This translation will be valid only for packets that are forwarded out from the NAT router into this domain.

Instructions: For static translation types unidirectional or SDPT, accept the default domain name, Public. Otherwise, specify a domain name for a network that is connected to a NAT router interface. The domain name must be in accordance with RFC 1035.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.9

Parameter: Static Nexthop

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > Bidirectional

Default: 0.0.0.0

Options: Any IP address

Function: Specifies the IP address of the next hop for this static translation.

Instructions: Enter the IP address of an interface that is directly connected to the NAT router. This address must be in the same subnet as the Source Domain. A value of 0.0.0.0 means that there is no Static Nexthop address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.10

Parameter: Unnumbered CCT Name

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > Bidirectional

Default: None

Options: Any unnumbered circuit name

Function: Specifies that this static translation occurs over this unnumbered interface.

Instructions: If you have not configured any unnumbered interfaces, leave this parameter blank. Otherwise, specify the appropriate circuit name from the list of configured unnumbered circuits. To view a list of the available unnumbered circuits, click on Values. The Unnumbered CCT Name parameter is supported for unidirectional NAT only.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.11

Adding NAT SDPT Parameters

To configure NAT static destination port translation (SDPT), set the following parameters:

Parameter: Private Address

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > SDPT

Default: None

Options: Any IP address of a host in the domain named Private

Function: For this SDPT translation, specifies the private address of a host in the domain named Private.

Instructions: Enter the appropriate IP address in dotted-decimal notation.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.3

Parameter: Private Port

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > SDPT

Default: None

Options: Any port number configured for UDP or TCP of a host in the domain named Private

Function: For this SDPT translation, specifies the private UDP or TCP port number of a host in the domain named Private.

Instructions: Enter the domain-specific port number.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.6

Parameter: Public Address

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > SDPT

Default: None

Options: Any registered IP address in a domain named Public

Function: For this SDPT translation, specifies a host address in a domain named Public.

Instructions: Enter the appropriate IP address in dotted-decimal notation.

MIB Object ID: Not available

Parameter: Public Port

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > SDPT

Default: None

Options: Any UDP or TCP port number

Function: For this SDPT translation, specifies a TCP or UDP port number in a domain named Public.

Instructions: Enter the translation port number.

MIB Object ID: Not available

Parameter: Protocol

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > SDPT
Default: TCP
Options: TCP | UDP
Function: Specifies the IP protocol type for this SDPT translation.
Instructions: Enter TCP or UDP, as appropriate.
MIB Object ID: Not available

Adding NAT Unidirectional Parameters

To configure static, unidirectional NAT, set the following parameters:

Parameter: Private Address

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > Unidirectional
Default: None
Options: IP address
Function: Specifies the original address for this static translation. Within a static mapping pair of addresses, this is the untranslated address.
Instructions: Enter the appropriate IP address in dotted-decimal notation.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.3

Parameter: Public Address

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > Unidirectional
Default: None
Options: Any IP address
Function: Specifies the public or external address for this static translation.
Instructions: Enter the appropriate IP address in dotted-decimal notation.
MIB Object ID: Not available

Parameter: Static Nexthop

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > Unidirectional

Default: 0.0.0.0

Options: Any IP address

Function: Specifies the IP address of the next hop for this static translation.

Instructions: Enter the IP address of an interface that is directly connected to the NAT router. This address must be in the same subnet as the Source Domain. A value of 0.0.0.0 means that there is no Static Nexthop address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.10

Parameter: Unnumbered CCT Name

Path: Configuration Manager > Protocols > IP > NAT > Static Mapping > **Add** > Unidirectional

Default: None

Options: Any unnumbered circuit name

Function: Specifies that this static translation occurs over this unnumbered interface.

Instructions: If you have not configured any unnumbered interfaces, leave this parameter blank. Otherwise, specify the appropriate circuit name from the list of configured unnumbered circuits. To view a list of the available unnumbered circuits, click on Values. The Unnumbered CCT Name parameter is supported for unidirectional NAT only.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.9.1.11

NAT Dynamic Mapping Parameters

To access the NAT dynamic mapping configuration windows (NAT Source Address Filter List and NAT Translation Pool List), complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **NAT**.	The NAT menu opens.
4. Choose **Dynamic Mapping**.	The Dynamic Mapping menu opens.
5. Choose **Source Address Filter.**	The NAT Source Address Filter List window opens.
6. Choose **Translation Pool**.	The NAT Translation Pool List window opens.

Depending on your configuration needs, go to the appropriate section:

Topic	Page
NAT Source Address Filter Parameters	A-25
NAT Translation Pool Parameters	A-31

NAT Source Address Filter Parameters

The following parameters are accessible from the NAT Source Address Filter List window:

Parameter: Enable

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter

Default: Enable

Options: Enable | Disable

Function: Enables or disables a source address filter. The NAT router checks the range of addresses in a configured source address filter to determine whether it will accept an address for translation.

Instructions: To enable the source address filter, set to Enable. To disable the source address filter, set to Disable. A source address filter must be enabled on the NAT router in order for dynamic address translation to occur.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.12.1.2

Parameter: Domain Name

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter

Default: None

Options: For unidirectional NAT: Private
For bidirectional NAT: any valid domain name for a network connected to a NAT router interface

Function: Specifies the domain name for which this source address filter is valid.

Instructions: For static translation types unidirectional or SDPT, accept the default value, Private. Otherwise, specify the domain name for a network connected to a NAT router interface that will be the source domain for this translation. The domain name must be in accordance with RFC 1035.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.12.1.7

Parameter: Translation Pool Selector

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter

Default: Outbound

Options: For unidirectional NAT: Outbound
For bidirectional NAT: Inbound or Outbound

Function: Specifies whether the translation pool is defined for the inbound (source) or the outbound (destination) domain. This value determines where to get the translation address for this source address filter.

Instructions: To specify that the translated address is from the source domain, specify Inbound. To specify that the translated address is from the destination domain, specify Outbound.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.12.1.8

Parameter: Nto1 Address

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter

Default: 0.0.0.0

Options: Any registered IP address

Function: Specifies the N-to-1 translation address used for this source address filter. (Think of this address as the “1” in the N-to-1 translation type. The “N” is the address range specified by the IP Address and Prefix Length parameters for the source address filter.)

Instructions: If you do not want to configure an N-to-1 translation, accept the default, 0.0.0.0. A value of 0.0.0.0 means that this is not an N-to-1 translation. If you want an N-to-1 translation, enter the registered IP address that you want to specify for translation by NAT.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.12.1.6

Parameter: Static Nexthop

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter

Default: 0.0.0.0

Options: Any IP address

Function: Specifies the IP address of the next hop for this dynamic translation.

Instructions: Enter the IP address of an interface that is directly connected to the NAT router. This address must be in the same subnet as the source domain. A value of 0.0.0.0 means that there is no Static Nexthop address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.12.1.9

Parameter: Unnumbered CCT Name

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter

Default: None

Options: Any unnumbered circuit name

Function: Specifies that this dynamic translation occurs over this unnumbered interface.

Instructions: If you have not configured any unnumbered interfaces, leave this parameter blank. Otherwise, specify the appropriate circuit name from the list of configured unnumbered circuits. To view a list of the available unnumbered circuits, click on Values. The Unnumbered CCT Name parameter is supported for unidirectional NAT only.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.12.1.10

Adding Source Address Filter Parameters

The following parameters are accessible when you click on the Add button from the NAT Source Address Filter List window, exposing the NAT Source Address Filter Add window:

Parameter: IP Address

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter > **Add**

Default: None

Options: IP address

Function: Together with the Prefix Length, specifies the range of addresses in a source address filter.

Instructions: Enter the appropriate IP address in dotted-decimal notation for the start of the range.

MIB Object ID: Not available.

Parameter: Prefix Length

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter > **Add**

Default: None

Options: 0 to 32 (decimal)

Function: Together with the starting IP Address, specifies the range of addresses in a translation pool. The prefix length indicates the network portion of the address range.

Instructions: Enter an integer from 1 through 32 that represents the number of contiguous bits in the network portion of the IP address. For example, the prefix length 24 for the address 197.1.1.0 sets the available addresses in the source address filter from 197.1.1.0 through 197.1.1.255.

MIB Object ID: Not available.

Parameter: Domain Name

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter > **Add**

Default: None

Options: For unidirectional NAT: Private
For bidirectional NAT: any valid domain name for a network connected to a NAT router interface

Function: Specifies the domain name for which this source address filter is valid.

Instructions: For static translation types unidirectional or SDPT, accept the default value, Private. Otherwise, specify the domain name for a network connected to a NAT router interface that is the source domain for this translation. The domain name must be in accordance with RFC 1035.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.12.1.7

Parameter: Translation Pool Selector

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter > **Add**

Default: Outbound

Options: For unidirectional NAT: Outbound
For bidirectional NAT: Inbound or Outbound

Function: Specifies whether the translation pool is defined for the inbound (source) or the outbound (destination) domain. This value determines where to get the translation address for this source address filter.

Instructions: To specify that the translated address is from the source domain, specify Inbound. To specify that the translated address is from the destination domain, specify Outbound.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.12.1.8

Parameter: Nto1 Address

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter > **Add**

Default: 0.0.0.0

Options: Any registered IP address

Function: Specifies the N-to-1 translation address used for this source address filter. (Think of this address as the "1" in the N-to-1 translation type. The "N" is the address range specified by the IP Address and Prefix Length parameters for the source address filter.)

Instructions: If you do not want to configure an N-to-1 translation, accept the default, 0.0.0.0. A value of 0.0.0.0 means that this is not an N-to-1 translation. If you want an N-to-1 translation, enter the registered IP address that you want to specify for translation by NAT.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.12.1.6

Parameter: Static Nexthop

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter > **Add**

Default: 0.0.0.0

Options: Any IP address

Function: Specifies the IP address of the next hop for this dynamic translation.

Instructions: Enter the IP address of an interface that is directly connected to the NAT router. This address must be in the same subnet as the source domain. A value of 0.0.0.0 means that there is no Static Nexthop address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.12.1.9

Parameter: Unnumbered CCT Name

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Source Address Filter > **Add**

Default: None

Options: Any unnumbered circuit name

Function: Specifies that this dynamic translation will occur over this unnumbered interface.

Instructions: If you have not configured any unnumbered interfaces, leave this parameter blank. Otherwise, specify the appropriate circuit name from the list of configured unnumbered circuits. To view a list of the available unnumbered circuits, click on Values. The Unnumbered CCT Name parameter is supported for unidirectional NAT only.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.12.1.10

NAT Translation Pool Parameters

The following parameters are accessible from the NAT Translation Pool List window:

Parameter: Enable

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Translation Pool

Default: Enable

Options: Enable | Disable

Function: Enables or disables a translation pool. The NAT router checks the range of addresses in a configured translation pool to determine whether it will accept an address for translation.

Instructions: To enable the translation pool, set to Enable. To disable the translation pool, set to Disable. A translation pool must be enabled on the NAT router in order for dynamic address translation to occur.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.13.1.2

Parameter: Domain Name

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Translation Pool

Default: Public

Options: For unidirectional NAT: Public
For bidirectional NAT: any valid domain name for a network connected to a NAT router interface

Function: Specifies the domain name for which this translation pool is valid.

Instructions: For unidirectional NAT, accept the default, Public. Otherwise, specify the domain name for a network connected to a NAT router interface for this translation pool. The domain name must be in accordance with RFC 1035.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.13.1.6

Adding NAT Translation Pool Parameters

The following parameters are accessible when you click on the Add button from the NAT Translation Pool List window, exposing the NAT Translation Pool Add window:

Parameter: IP Address

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Translation Pool > **Add**

Default: None

Options: IP address

Function: Together with the Prefix Length, specifies the range of addresses in a translation pool. NAT maps an address in the source domain to an address within this range.

Instructions: Enter the appropriate IP address in dotted-decimal notation for the start of the range. The address must be in the destination domain, whether Public or other.

MIB Object ID: Not available.

Parameter: Prefix Length

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Translation Pool > **Add**

Default: None

Options: 0 to 32 (decimal)

Function: Together with the starting IP Address, specifies the range of addresses in a translation pool. The prefix length indicates the network portion of the address range.

Instructions: Enter an integer from 1 through 32 that represents the number of contiguous bits in the network portion of the IP address. For example, the prefix length 24 for the address 197.1.1.0 sets the available addresses in the translation pool from 197.1.1.0 through 197.1.1.255.

MIB Object ID: Not available.

Parameter: Domain Name

Path: Configuration Manager > Protocols > IP > NAT > Dynamic Mapping > Translation Pool > **Add**

Default: For unidirectional NAT: Public
For bidirectional NAT: any valid domain name for a network connected to a NAT router interface

Options: For unidirectional NAT: Public
For bidirectional NAT: any valid domain name for a network connected to a NAT router interface

Function: Specifies the domain name for which this translation pool is valid.

Instructions: For unidirectional NAT, accept the default, Public. Otherwise, specify the domain name for a network connected to a NAT router interface for this translation pool. The domain name must be in accordance with RFC 1035.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.7.13.1.6

RIPSO Parameters

The IP Interface List window (Figure A-3) allows access to parameters that configure RIPSO on a router interface.

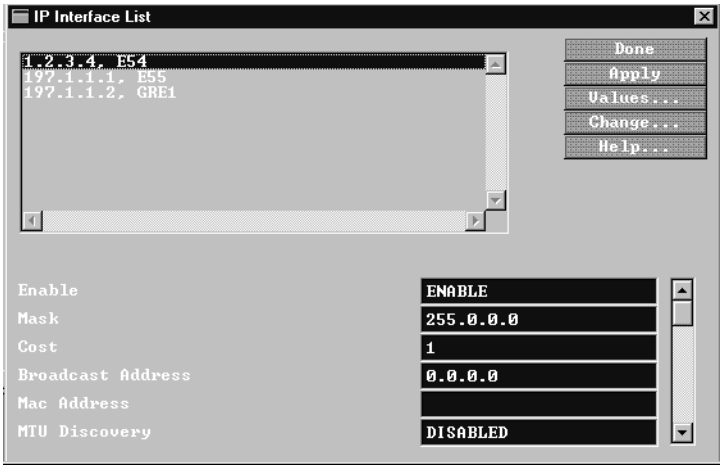


Figure A-3. IP Interface List Window

To access the IP Interface List window, complete the following tasks:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IP**.	The IP menu opens.
3. Choose **Interfaces**.	The IP Interface List window opens.
4. Click on the interface that you want to edit.	Site Manager displays the parameter values for that interface.

Parameter: Enable Security

Path: Configuration Manager > Protocols > IP > Interfaces

Default: Enable

Options: Enable | Disable

Function: Enables or disables IP security options for this interface.

Instructions: Set to Disable if you want to disable IP security options. If you set this parameter to Disable, the router accepts only the following IP datagrams: labeled IP datagrams with the classification level set to Unclassified and no authority flags set, and unlabeled IP datagrams.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.76

Parameter: Strip Security

Path: Configuration Manager > Protocols > IP > Interfaces

Default: None

Options: None | Incoming | Outgoing | All

Function: Specifies the type of IP datagram from which the router should remove the IP security options.

Instructions: Select the type of IP datagram from which you want IP security options to be removed. None causes the router to leave IP security options on all inbound and outbound IP datagrams intact. Incoming causes the router to strip the IP security option from each incoming IP datagram after checking the IP datagram against the interface's security configuration. Outgoing causes the router to strip the IP security option from each outgoing IP datagram before checking each datagram against the interface's security configuration. All causes the router to strip the IP security options from both incoming and outgoing IP datagrams: incoming datagrams after checking each against this interface's security configuration and outgoing datagrams before checking each against the interface's security configuration. If you set this parameter to Outgoing or All, then you must set the Require Out Security parameter to None. (Similarly, if you set the Require Out Security parameter to Forwarded, Originated, or All, then you must set this parameter to None or Incoming.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.77

Parameter: Require Out Security

Path: Configuration Manager > Protocols > IP > Interfaces

Default: All

Options: None | Forwarded | Originated | All

Function: Specifies which type of outbound datagrams require IP security labels.

Instructions: Select None: the router forwards unlabeled IP datagrams unchanged on this interface. In addition, those IP datagrams that it originates and transmits do not require labels. Select Forwarded: the router requires all IP datagrams that it forwards on this interface (not those it originates) to contain basic IP security options. If the datagram already contains an IP security label, the router forwards the datagram unchanged. If the datagram is unlabeled, the router adds the implicit or default label to the datagram before forwarding it. Select Originated: the router specifies basic IP security options for all IP datagrams that it originates and transmits on this interface. The router adds the default label to IP datagrams that it originates and transmits on this interface. Select All: the router requires all datagrams (both those that it forwards and those it originates) on this interface to contain basic IP security options. It supplies the implicit or default label for those datagrams that do not already contain one. If you set this parameter to Originated or All, you must enable the Default Label and Error Label parameters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.78

Parameter: Require In Security

Path: Configuration Manager > Protocols > IP > Interfaces

Default: All

Options: None | All

Function: Specifies which type of incoming IP datagram requires security labels.

Instructions: Select None: the router does not require inbound IP datagrams to contain labels. Select All: the router requires all inbound IP datagrams received on this interface to contain basic IP security options.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.79

Parameter: Minimum Level

Path:	Configuration Manager > Protocols > IP > Interfaces
Default:	Unclassified
Options:	Unclassified | Confidential | Secret | Top Secret
Function:	Specifies the minimum security level that the router allows for inbound or outbound IP datagrams. This parameter, together with the Maximum Level parameter, specifies the range of classification levels that the router will accept and process. The router drops IP datagrams received on this interface that are below the specified minimum level.
Instructions:	Select a minimum security level for this interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.4.80

Parameter: Maximum Level

Path:	Configuration Manager > Protocols > IP > Interfaces
Default:	Top Secret
Options:	Unclassified | Confidential | Secret | Top Secret
Function:	Specifies the maximum security level that the router allows for inbound or outbound IP datagrams. This parameter, together with the Minimum Level parameter, specifies the range of classification levels that the router accepts. The router drops IP datagrams it receives or transmits on this interface that are above the specified maximum level.
Instructions:	Select a maximum security level for this interface. The maximum level must be greater than or equal to the minimum level.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.4.81

Parameter: Must Out Authority

Path: Configuration Manager > Protocols > IP > Interfaces

Default: No authority flags selected

Options: No authority flags selected | GENSER | SIOPESI | SCI | NSA | DOE

Function: Specifies which authority flags must be set in the protection authority field of all outbound datagrams.

Instructions: Select all authority flags that the router must set in all outbound IP datagrams that it transmits on this interface. If you do not select any authority flags (the default setting), the router does not set any protection authority flags in outbound IP datagrams.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.82

Parameter: May Out Authority

Path: Configuration Manager > Protocols > IP > Interfaces

Default: Any

Options: Any | GENSER | SIOPESI | SCI | NSA | DOE

Function: Specifies which authority flags may be set in the protection authority field of all outbound datagrams. The authority flags that you specify here must be a superset of the authority flags that you specify for the Must Out Authority parameter.

Instructions: The default setting specifies that any of the authority flags may be set. Either accept the default setting or reset and select only those authority flags that are appropriate.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.83

Parameter: Must In Authority

Path: Configuration Manager > Protocols > IP > Interfaces

Default: No authority flags selected

Options: No authority flags selected | GENSER | SIOPESI | SCI | NSA | DOE

Function: Specifies which authority flags must be set in the protection authority field of inbound IP datagrams.

Instructions: Select all authority flags that must be set in inbound IP datagrams received on this interface. If you do not select any authority flags (the default setting), then the router does not require a datagram to have authority flags set, but still accepts the datagram if any flags are set.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.84

Parameter: May In Authority

Path: Configuration Manager > Protocols > IP > Interfaces

Default: Any

Options: Any | GENSER | SIOPESI | SCI | NSA | DOE

Function: Specifies which authority flags may be set in the protection authority field of inbound IP datagrams. The authority flags that you specify here must be a superset of the authority flags that you specify for the Must In Authority parameter.

Instructions: The default setting specifies that any of the authority flags may be set. Either accept the default setting or reset and select only those authority flags that are appropriate.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.85

Parameter: Implicit Label

Path: Configuration Manager > Protocols > IP > Interfaces

Default: Enable

Options: Enable | Disable

Function: If you select Enable, the router uses the Implicit Authority and Implicit Level fields to create an implicit label. The router supplies the implicit label to unlabeled inbound datagrams received by this interface. If you select Disable, the router does not supply implicit labels for this interface.

Instructions: Accept the default, Enable, to allow the router to supply implicit labels for unlabeled inbound datagrams.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.86

Parameter: Implicit Authority

Path: Configuration Manager > Protocols > IP > Interfaces

Default: No authority flags selected

Options: No authority flags selected | GENSER | SIOPESI | SCI | NSA | DOE

Function: Specifies the authority flags that the router sets when it supplies implicit security labels for unlabeled inbound IP datagrams.

Instructions: Select all authority flags that the router should set when it supplies an implicit security label. The set of authority flags that you specify here must include the set of authority flags that you specified for the Must In Authority parameter, and cannot include any of the flags that you did not specify for the May In Authority parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.87

Parameter: Implicit Level

Path:	Configuration Manager > Protocols > IP > Interfaces
Default:	Unclassified
Options:	Unclassified | Confidential | Secret | Top Secret
Function:	Specifies the security level that the router sets when it supplies implicit security labels for unlabeled, inbound IP datagrams.
Instructions:	Specify a level within the range specified by the Minimum Level and Maximum Level parameters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.4.88

Parameter: Default Label

Path:	Configuration Manager > Protocols > IP > Interfaces
Default:	Enable
Options:	Enable | Disable
Function:	If you select Enable, the router uses the Default Authority and Default Level fields to create a default label. The router supplies the default label to unlabeled outbound datagrams originated or forwarded out this interface. If you select Disable, the router does not supply default labels for this interface.
Instructions:	To allow the router to supply default labels for unlabeled outbound datagrams, accept the default, Enable.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.4.89

Parameter: Default Authority

Path:	Configuration Manager > Protocols > IP > Interfaces
Default:	No authority flags selected
Options:	No authority flags selected | GENSER | SIOPESI | SCI | NSA | DOE
Function:	Specifies the authority flags that the router uses when it supplies default security labels to unlabeled outbound IP datagrams.
Instructions:	Select authority flags that the router should set when it supplies default security labels. The set of authority flags that you specify must include the set of authority flags specified for the Must Out Authority parameter, and cannot include any of the flags that you did not specify for the May Out Authority parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.4.90

Parameter: Default Level

Path:	Configuration Manager > Protocols > IP > Interfaces
Default:	Unclassified
Options:	Unclassified | Confidential | Secret | Top Secret
Function:	Specifies the security level that the router sets when it supplies default security labels to unlabeled outbound IP datagrams.
Instructions:	Specify a default level within the range specified by the Minimum Level and Maximum Level parameters.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.2.1.4.91

Parameter: Error Label

Path: Configuration Manager > Protocols > IP > Interfaces

Default: Enable

Options: Enable | Disable

Function: If you select Enable, the router uses the Error Authority and Minimum Level fields to create an error label. The router supplies the error label to outbound ICMP error datagrams. If you select Disable, the router does not supply error labels for this interface.

Instructions: To allow the router to supply error labels for outbound ICMP error datagrams, accept the default, Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.92

Parameter: Error Authority

Path: Configuration Manager > Protocols > IP > Interfaces

Default: No authority flags selected

Options: No authority flags selected | GENSER | SIOPESI | SCI | NSA | DOE | ALL

Function: Specifies the authority flags that the router uses when it supplies error security labels to outbound ICMP error datagrams.

Instructions: Select authority flags that the router should set when it supplies error security labels to outbound ICMP error datagrams. The set of authority flags that you specify here must include the set of authority flags that you specified for the Must Out Authority parameter, and cannot include any of the flags that you did not specify for the May Out Authority parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.93

Appendix B
Sample Bidirectional NAT Configuration

PROBLEM: Hosts in two domains at your site need to share information, yet you need to keep the source and destination addresses of these IP packets hidden from each of these hosts.

SOLUTION: You configure dynamic bidirectional NAT on a router, hereafter referred to as *the NAT router*, between these two domains.

Overview of Configuration Tasks

To configure dynamic bidirectional NAT, you must configure the following:

- DNS server software on a device accessible to the NAT router
- On the NAT router, an interface to each domain with the following services:
  - -- IP
  - -- RIP (or static route to the next device in an individual domain)
  - -- DNS proxy
  - -- NAT
- On the NAT router, a *source address filter* (addresses matching this filter are translated by NAT) and *translation pool* (NAT uses this pool of addresses from which to get a translation addresses for source or destination addresses that match an enabled source address filter).
- DNS client on hosts in both domains (These hosts send IP traffic into the NAT router. Any source or destination addresses that match an enabled source address filter are translated by NAT.)
- RIP or static routes between devices in the domains serviced by the NAT router

The configuration tasks are similar when configuring *static bidirectional NAT*, except that you have the option of choosing whether or not to put DNS proxy on the NAT router.

Sample Scenario

In the BayRS implementation of NAT, a *domain* is a network of devices with uniquely assigned IP addresses, such that datagrams can be routed among them. The domains in this scenario are domain1.net and domain2.net.

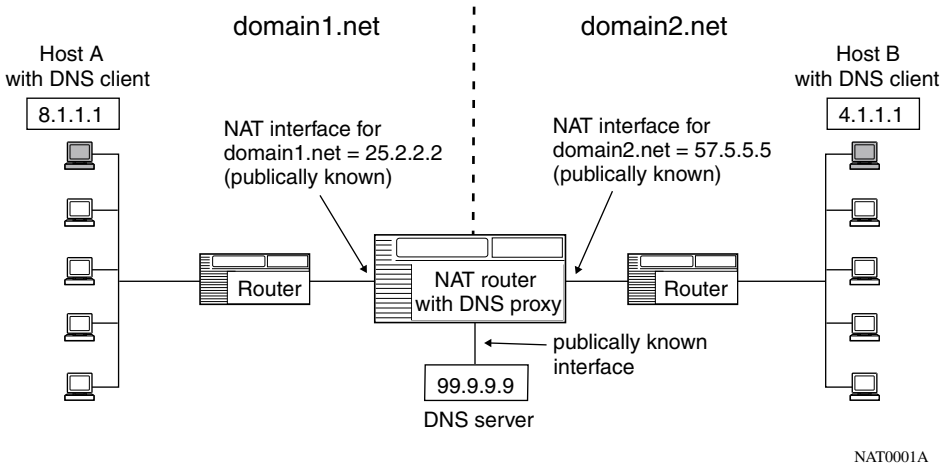


Figure B-1. Sample Configuration for Bidirectional NAT

Looking at Figure B-1, as an IP packet travels from host A in domain1.net, its source address is hidden from host B in domain2.net when the NAT router supplies a translation address based on the configured translation pool. When the NAT router discerns that the destination address matches a source address filter, NAT replaces this address with one in the translation pool for this source address filter in domain2.net.

A similar translation process occurs when host B in domain2.net initiates traffic to host A in domain1.net, when the NAT router translates the source address and destination address for IP traffic from Host B that matches a configured source address filter. So, bidirectional NAT translates both the source and destination address for IP traffic travelling from host A to host B or from host B to host A.

The address translation at the NAT router occurs with the assistance of BayRS DNS proxy on the router and a public interface to a DNS server (99.9.9.9). The DNS proxy server accepts DNS name service requests from hosts A and B (each configured with DNS client) and forwards these requests to the preconfigured external DNS server.

When a DNS reply comes back, the DNS proxy server queries NAT services and NAT queries the destination domain to determine whether the address needs to be translated, based on the enabled source address filters. NAT then supplies translated addresses to the DNS proxy server. NAT dynamically assigns the next available, lowest IP address from the applicable translation pool.

Configuring Sample Bidirectional NAT Using the BCC

The following instructions for configuring dynamic bidirectional NAT using the BCC are based on the scenario shown in Figure B-1 on page B-2. You could create this same configuration using Site Manager. For instructions on configuring bidirectional NAT using Site Manager, see page 2-56.

Information Used in Bidirectional NAT Configuration

Before you proceed with your configuration, you should map out some address information for each domain, including the NAT router interface, the source address filter range, the translation pool range, and the address of the DNS server (Table B-1). In your configuration, a single domain may have more than one of any of these items. Preparing this information will make your configuring go more smoothly.

Table B-1. Information to Gather Before Configuring NAT

	Domain1.net	Domain2.net
NAT router interface for this domain (in this scenario, this interface will also be configured with IP, RIP2, and DNS proxy)	25.2.2.2	57.5.5.5
Source Address Filter	8.0.0.0/8	4.0.0.0/8
Translation Pool	192.1.0.0/24	138.5.0.0/16
DNS server for NAT router	99.9.9.9	99.9.9.9

1. **Configure a DNS server with a public address on the same network as the router to be configured with NAT. For instructions, consult your third-party DNS server supplier.**

   You can assign up to three such servers for use with bidirectional NAT.

   For this sample configuration, presume that a single DNS server has been configured on a device at IP address 99.9.9.9.

2. **On the router to be configured with NAT, configure IP on an interface for each domain.**

   At a minimum, you must configure one interface for each domain.

   Configuring router interface 25.2.2.2 with IP for domain1.net and interface 57.5.5.5 with IP for domain2.net:

```
box# ethernet slot 2 connector 2
ethernet/2/2# ip 25.2.2.2/8
ip/25.2.2.2/255.0.0.0# back
ethernet/2/2# back
box# eth 2/3
ethernet/2/3# ip 57.5.5.5/8
```

   To view the status of the IP interfaces on the router, use the **show ip interfaces** *command:*

```
ip/57.5.5.5/255.0.0.0# show ip interfaces

Circuit       Circuit # State     IP Address    Mask          MAC Address
-------------------------------------------------------------------------
E22           1         up        25.2.2.2      255.0.0.0     0
E23           3         up        57.5.5.5      255.0.0.0     0
```

3. **On the router to be configured with NAT, configure RIP2 on an interface for each domain.**

   Use the same interfaces for which you have configured IP. At a minimum, you must configure one RIP interface for each domain.

   Alternatively, you can you specify the next hop from the router interface to the next device in a domain using the NAT next-hop-address parameter (accessible when you are configuring a source address filter, step 6 herein). Configuring the next-hop address parameter lets you omit running RIP on the NAT router. If you use the next-hop-address parameter, you must also configure a static route from the next hop device to an adjacent host.

Configuring RIP2 on the router IP interface 25.2.2.2 for domain1:

```
ip/25.2.2.2/255.0.0.0# rip
rip/25.2.2.2# version rip2
```

Configuring RIP2 on the router IP interface 57.5.5.5 for domain2:

```
ip/57.5.5.5/255.0.0.0# rip
rip/57.5.5.5# version rip2
```

To view the status of RIP on the router, enter the **show ip rip enabled** *command:*

```
rip/57.5.5.5# show ip rip enabled
                                        Def.
                                RIP     Rt.       Poison   RIP   Trig.
IP Interface    Cct# State      Sup/Lis Sup/Lis   Reverse  Mode  Updates  TTL
--------------- ---- ---------- ------- -------   -------- ----- -------- ---
25.2.2.2        1    up         ena/ena dis/dis    poisoned  rip2  disabled 1
                                ble ble abl abl
                                d   d   ed  ed
57.5.5.5        3    up         ena/ena dis/dis    poisoned  rip2  disabled 1
                                ble ble abl abl
                                d   d   ed  ed
```

4. On the router to be configured with NAT, configure DNS proxy on an interface for each domain.

Use the same interfaces for which you have configured IP and RIP. Navigate to the IP interface prompt for a publically known interface of the NAT router that is in the same network as your first domain (domain1.net) and enter the DNS proxy command. Then, configure the DNS proxy parameters domain-name, fwd-server1-address, and mode (*nat_translation*). You can specify up to three forwarding servers total, but this sample shows only the one configured at 99.9.9.9. Accept default values for the rest of the DNS proxy parameters. At a minimum, you must configure one DNS proxy interface for each domain.

Configuring DNS proxy on the router IP interface 25.2.2.2 for domain1.net:

```
ip/25.2.2.2/255.0.0.0# dns-proxy
dns-proxy/25.2.2.2# domain-name domain1.net
dns-proxy/25.2.2.2# fwd-server1-address 99.9.9.9
dns-proxy/25.2.2.2# mode nat-translation
dns-proxy/25.2.2.2# info
   answer-truncation disabled
   domain-name domain1.net
```

```
   fwd-port 53
   fwd-server1-address 99.9.9.9
   fwd-server2-address 0.0.0.0
   fwd-server3-address 0.0.0.0
   max-answers-truncated 1
   max-cache-size 20
   max-queries-allowed 20
   max-retransmissions 2
   mode nat-translation
   port 53
   state enabled
   timeout 5
dns-proxy/25.2.2.2#
```

Configuring DNS proxy on the router IP interface 57.5.5.5 for domain2.net:

```
ip 57.5.5.5/255.0.0.0# dns-proxy
dns-proxy/57.5.5.5# domain-name domain2.net
dns-proxy/57.5.5.5# fwd-server1-address 99.9.9.9
dns-proxy/57.5.5.5# mode nat-translation
```

5. **On the router to be configured with NAT, configure NAT on an interface for each domain.**

   Use the same interfaces for which you have configured IP, RIP, and DNS proxy and specify the domain name with which it is associated. At a minimum, you must configure one NAT interface for each domain.

   Configuring NAT on the router IP interface 25.2.2.2 for domain1:

```
ip/25.2.2.2/255.0.0.0# nat domain-name domain1.net
nat/25.2.2.2# info
   domain-name domain1.net
   state enabled
```

   Configuring NAT on the router IP interface 57.5.5.5 for domain2:

```
ip 57.5.5.5/255.0.0.0# nat domain-name domain2.net
ip 57.5.5.5/255.0.0.0# info
   domain-name domain2.net
   state enabled
```

To view the status of the NAT interfaces on the router, enter the **show nat interfaces** *command:*

```
IP              Circuit Domain                        Packets        Drop
Address         Name    Name                  Tx                  Rx Count
--------------- ------- -------------------- -------------------- ----------
25.2.2.2        E22     domain1.net          0                    0          0
57.5.5.5        E23     domain2.net          0                    0          0
```

6. **Configure a source address filter for each domain that will use the NAT router for address translation of IP packets.**

   Navigate to the NAT global prompt such as **box; ip; nat**, and configure the domain name, then configure a source address filter for the domain by specifying an IP address and prefix length. Accept default values for the other parameters. At a minimum, you must configure one NAT source address filter for each domain.

   Note that the default value for which translation pool to use with a source address filter is the translation pool of the outbound domain. If this value were set to inbound, the translation pool would be from the same domain as the source address filter.

   Configuring a source address filter for domain1.net:

```
nat# domain domain1.net
domain/domain1.net# src-filter 8.0.0.0/8
src-filter/8.0.0.0/8/domain1.net# info
   n-to-1 0.0.0.0
   next-hop-address 0.0.0.0
   prefix-length 8
   start-address 8.0.0.0
   state enabled
   type 1-to-1
   unnumbered-circuit-name {}
   use-translation-pool outbound
```

   Configuring a source address filter for domain2.net:

```
nat# domain domain2.net
domain/domain1.net# src-filter 4.0.0.0/8
src-filter/4.0.0.0/8/domain1.net#
```

To check the addresses in a source address filter and to see whether a source address filter is enabled or disabled, use the **show nat filters** *command:*

```
src-filter/8.0.0.0/8/domain1.net# show nat filters

       Filter Address Range       Pre          Domain
Starting                  Ending fix State    Name
--------------------------------- --- -------- --------------------------------
8.0.0.0             8.255.255.255   8 enabled  domain1.net
4.0.0.0             4.255.255.255   8 enabled  domain2.net
```

7. **Configure a translation pool for each domain that will use the NAT router for address translation of IP packets.**

   Navigate to the NAT global prompt such as **box; ip; nat**, and identify the domain name, then configure a translation pool for the domain by specifying an IP address and prefix length. Accept default values for the other parameters. At a minimum, you must configure one NAT source address filter for each domain.

   Configuring a translation pool for domain1.net:

   ```
   nat# domain domain1.net
   domain/domain1.net# trans-pool 192.1.0.0/24
   trans-pool/192.1.0.0/24/domain1.net# info
      prefix-length 24
      start-address 192.1.1.1
      state enabled
   ```

   Configuring a translation pool for domain2.net:

   ```
   nat# domain domain2.net
   domain/domain2.net# trans-pool 138.5.0.0/16
   trans-pool/138.5.0.0/16/domain2.net#
   ```

   To check translation pool address ranges and to see whether a translation pool is enabled or disabled, use the **show nat pools** *command:*

```
nat# show nat pools

       Pool Address Range         Pre          Domain
Starting                  Ending fix State    Name
--------------------------------- --- -------- --------------------------------
192.1.1.1           192.1.1.255   24  enabled  domain1.net
138.5.0.0           138.5.255.255 16  enabled  domain2.net
```

8. **Configure DNS client on each device in the domains that will initiate IP traffic whose addresses will be translated by the NAT router. For instruction, consult your third-party DNS client supplier.**

   For the server address, specify the IP address of the NAT router interface for that domain.

   Configuring DNS client on a non-NAT router in domain1:

```
box# dns
dns# domain-name domain1.net
dns# name-server 1 address 25.2.2.2
name-server/1#
```

   Configuring DNS client on a non-NAT router in domain2:

```
box# dns
dns# domain-name domain2.net
dns# name-server 1 address 57.5.5.5
name-server/1#
```

9. **Configure RIP2 on or static routes between each device that will pass IP packets whose source and destination addresses will be translated by the NAT router.**

Checking Address Translations

After you configure your router for bidirectional NAT, you can use various **show nat** commands to check NAT, whether from the BCC or from the Technician Interface.

Table B-2. Available show nat Commands

This show nat option	Is available using the:	
	BCC	Technician Interface
base		✓
domains	✓	✓
filters	✓	✓
interfaces	✓	✓
mappings	✓	
pools	✓	✓
sdpt		✓
summary	✓	
translations		✓
version		✓

For instance, the BCC **show nat summary** command displays the following NAT router global parameter information: NAT state, soloist slot, dynamic aging, dynamic timer, translations dynamic, translations FTP, and install private addresses.

Examples of the BCC **show nat filters**, **show nat interfaces**, and **show nat pools** commands can be found in the section "Configuring Sample Bidirectional NAT Using the BCC," starting on page B-3. Examples of the **show nat domains** (BCC), **show nat mappings** (BCC), and **show nat translations** (Technician Interface) follow.

For more information on the BCC show nat commands, see *Reference for the BCC IP show Commands*. In addition to using show commands to monitor NAT, you can capture NAT debug messages in log files. For instructions, see "Logging NAT Messages" on page 2-69.

show nat domains (BCC)

The command **show nat domains** displays address translations for the domains used in NAT. You can use the following filters with this command: **-in-domain** *<dname>*, **-out-domain** *<dname>*, and **-address** *<IP_address>* .

Using the sample configuration, if you sent a ping from host A to host B and one from one B to host A then issued the **show nat domains** command, you would see:

```
nat# show nat domains

Original        Translated      Inbound                 Outbound
IP Address      IP Address      Domain                  Domain
--------------- --------------- ----------------------- -----------------------
8.1.1.1          138.5.0.1       domain1.net             domain2.net
4.1.1.1          138.5.0.2       domain2.net             domain2.net
8.1.1.1          192.1.0.1       domain1.net             domain1.net
4.1.1.1          192.1.0.2       domain2.net             domain1.net
```

In this output of the NAT router:

- The first translation is for host A (8.1.1.1) in the inbound domain (domain1.net) getting the first available address (138.5.0.1) from the translation pool (138.5.0.0/16) of the outbound domain (domain2.net). Remember that the source address filter for the host domain (domain1.net) is set by default in NAT to use the translation pool of the outbound domain (here, domain2.net).
- The second translation is the result of host B (4.1.1.1) making a DNS client address request of the DNS proxy server on the NAT router. NAT replaces the address information in the packet with the next available address (138.5.0.2) from the translation pool (138.5.0.1/16) from host B's own domain (domain2.net).
- The third translation is the result of host A (8.1.1.1) making a DNS client address request of the DNS proxy server on the NAT router. NAT replaces the address information in the packet with the next available address (192.1.0.1) from the translation pool (192.1.0.0/24) from host A's own domain (domain1.net).

- The fourth translation is for host B (4.1.1.1) in the inbound domain (domain2.net) getting the first available address (192.1.0.2) from the translation pool (192.1.0.1/24) of the outbound domain (domain1.net). Remember that the source address filter for the host domain (host B's domain is domain2.net) is set by default in NAT to use the translation pool of the outbound domain (domain1.net).

show nat mappings (BCC)

To check current address mappings in the NAT table on the router, use the **show nat mappings** command. For each translation, this command reports the number of packets sent and received. You can use the following filters with this command: **-in-domain** *<dname>*, **-out-domain** *<dname>*, **-address** *<IP_address>* and **type** (displays whether the mapping is 1-to1, static, or n-to-1.

Using addresses from the previous sample configuration, if you sent a ping from host A to host B and issued the **show nat mappings** command, the results would be similar to the following:

```
nat# show nat mappings

Original        Translated      IP    Orig  Trans        Packets        Last
IP Address      IP Address      Proto Port  Port  Tx                 Rx Used
--------------- --------------- ----- ----- ----- -------------------- --------
8.1.1.1          138.5.0.1     none     0     0    1                1   80
8.1.1.1          192.1.0.1     none     0     0    1                1   80
4.1.1.1          192.1.0.2     none     0     0    1                1   80
```

- The first translation shown is host A (8.1.1.1) using a translated address (138.5.0.1) from the translation pool (138.5.0.0/16) of the outbound domain (domain2.net).
- The second translation is the result of host A (8.1.1.1) making a DNS client address request of the DNS proxy server. The NAT router replaces the address information in the packet with a translated address (192.1.0.1) from the translation pool (192.1.0.0/24) from host A's domain (domain1.net).
- The third translation shows the NAT router translating the address of host B (4.1.1.1) using the next available address (192.1.0.2) in the translation pool (192.1.0.0/24) in the domain which is outbound (domain1.net) of host B's domain (domain2.net).

- The output columns IP Protocol (UDP, TCP, or none are possible values), Original Port, and Translated Port are specific to NAT SDPT, not bidirectional NAT.

If you then did a ping from host B to host A and followed with a **show nat mappings** command, you would see output similar to the following:

```
nat# show nat mappings

Original        Translated      IP    Orig  Trans        Packets        Last
IP Address      IP Address      Proto Port  Port  Tx                Rx Used
--------------- --------------- ----- ----- ----- ------------------- --------
8.1.1.1          138.5.0.1     none     0     0    2                2   120
4.1.1.1          138.5.0.2     none     0     0    1                1   120
8.1.1.1          192.1.0.1     none     0     0    1                1   120
4.1.1.1          192.1.0.2     none     0     0    2                2   120
```

Notice the addition of the second line here, which reports the result of Host B (4.1.1.1) making a DNS client address request of the DNS proxy server on the NAT router. NAT replaces the address information in the DNS packet with a translated address from the translation pool (138.5.0.1) from host B's own domain (domain2.net). Notice, too, the update in the number of packets sent and received; this indicates the additional ping from host B to host A.

show nat translations (Technician Interface)

The Technician Interface script **show nat translations** is also helpful for monitoring NAT router packet translations. For example:

```
$> show nat translations
NAT ADDRESS TRANSLATION STATISTICS
----------------------------------

                                ORIG   TRANS  TRANS
ORIGINAL ADDR   TRANSLATED ADDR PORT   PORT   TYPE   TIMEOUT OCTETS RX OCTETS TX
--------------  --------------- -----  -----  -----  ------- --------- ---------
8.1.1.1          138.5.0.1          0      0     DYN       5         2         2
4.1.1.1          138.5.0.2          0      0     DYN       5         1         1
8.1.1.1          192.1.0.1          0      0     DYN       5         1         1
4.1.1.1          192.1.0.2          0      0     DYN       5         2         2

TOTAL of  4  entry(s)
```

The output columns Original Port and Translated Port display port number information specific to NAT SDPT, not bidirectional NAT.

Index

A

accept policies, configuring for GRE tunnels, 1-7, 1-8

acronyms, xvii

address translation precedence (NAT), 2-35

aging (NAT), enabling/disabling timer, 2-71

announce policies, configuring for GRE tunnels, 1-7

Area Address parameter (OSI), 1-15

authority flags (RIPSO)
- inbound datagrams, 3-12
- outbound datagrams, 3-11

authority values (RIPSO), 3-4

B

BFE support
- addressing, 4-4
- configuring, 4-5
- logical address limitation, 4-4
- overview, 4-2
- subaddress limitation, 4-4
- X.25 packet-level parameter settings for, 4-6
- X.25 service-level parameter settings for, 4-8

BGP support limitation for NAT, 2-33

bidirectional multidomain NAT. *See* bidirectional NAT

bidirectional NAT
- advantages, 2-7
- BGP support limitation, 2-33
- defined, 2-7
- DNS client requirement, 2-8
- DNS proxy
  - considerations, 2-87
  - requirement for dynamic, 2-8
- DNS server requirement, 2-8
- dynamic translation (walkthrough), 2-50, B-3
- ECMP support limitation, 2-33
- how dynamic translation works, 2-28
- how static translation works, 2-26
- IPsec support limitation, 2-34
- OSPF support limitation, 2-33
- public router interfaces, 2-32
- requirements, 2-7
- static mapping, 2-84
- three domains, 2-29
- two domains, 2-28

Blacker Front-End. *See* BFE support

C

Circuit Password parameter (OSI), 1-15

circuitless IP address, using as GRE tunnel interface, 1-4

configuring
- BFE support, 4-1
- GRE tunnels, 1-10
- NAT, 2-40
- RIPSO, 3-1

Connection Name parameter (GRE), 1-19, 1-20, A-5

conventions, text, xvi

customer support, xix

D

Default Authority parameter (RIPSO), 3-14, A-42

Default Label parameter (RIPSO), 3-14, A-41

default labels (RIPSO)
- defined, 3-5
- enabling or disabling use of, 3-14

Default Level parameter (RIPSO), 3-14, A-42

delete command (BCC)
GRE
remote tunnel end point, 1-26
tunnel, 1-27
tunnel protocol, 1-24
NAT
from a router interface, 2-79
source address filter, 2-105
static address mapping, 2-93
translation pool, 2-111
deleting
GRE
remote tunnel end point, 1-26
tunnel, 1-27
tunnel protocol, 1-24
NAT
from an interface, 2-79
from the router, 2-79
source address filter, 2-105
static address mapping, 2-93
translation pool, 2-111
Destination Domain parameter (NAT)
static address mapping, A-15
static bidirectional, 2-88, A-19
disabling
GRE
remote tunnel end point, 1-25
tunnel, 1-21
tunnel protocol, 1-22
NAT
on an interface, 2-77
on the router, 2-66
source address filter, 2-103
static address mapping, 2-92
translation pool, 2-109
RIPSO
error labeling, 3-15
labeling for unlabeled outbound datagrams, 3-14
on an interface, 3-6
DNS client
bidirectional NAT requirement, 2-8
using Site Manager to configure, 2-63
using the BCC to configure, 2-52
DNS proxy
dynamic bidirectional NAT requirement, 2-8
static bidirectional NAT considerations, 2-87
timeout considerations, 2-53
using Site Manager to configure, 2-59
using the BCC to configure, 2-53
DNS server
bidirectional NAT requirement, 2-8
installing for bidirectional NAT, 2-51, 2-56
domain (NAT)
defined, 2-2
number of router interfaces to each, 2-32
domain name (NAT)
bidirectional, 2-8
private, 2-3
public, 2-3
requirements, 2-52
unidirectional, special, 2-3
Domain Name parameter (NAT)
interface, A-12
N-to-1, 2-114
source address filter, 2-98, 2-102, A-25, A-29
translation pool, 2-108, A-32, A-33
dynamic translations (NAT)
address range considerations, 2-11
bidirectional (walkthrough), 2-50
comparison of unidirectional and bidirectional, 2-12
configuring, 2-95
defined, 2-10
DNS proxy requirement, 2-8
how bidirectional NAT works, 2-28
how unidirectional NAT works, 2-15
mapping aging, enabling timer, 2-71
overview, 2-11
port (N-to-1), 2-113
source address filter
adding, 2-97
address range considerations, 2-98
deleting, 2-105
disabling, 2-103
enabling, 2-103
reenabling, 2-103
translation pool
adding, 2-106
deleting, 2-111
disabling, 2-109
enabling, 2-109
reenabling, 2-109
unidirectional (walkthrough), 2-40

E

ECMP support limitation for NAT, 2-33

Enable parameter
- GRE
  - remote tunnel end point, 1-26, A-5
  - tunnel, 1-22, A-4
- NAT
  - global, 2-66, A-8
  - interface, 2-78, A-11
  - source address filter, 2-104, A-25
  - static address translation, 2-93, A-13
  - translation pool, 2-110, A-31
- OSI, 1-15

Enable Security parameter (RIPSO), 3-6, A-35

enabling
- GRE
  - remote tunnel end point, 1-25
  - tunnel, 1-21
  - tunnel protocol, 1-22
- NAT
  - on an interface, 2-77
  - on the router, 2-66
  - source address filter, 2-103
  - static address mapping, 2-92
  - translation pool, 2-109
- RIPSO
  - error labeling, 3-15
  - labeling for unlabeled outbound datagrams, 3-14
  - on an interface, 3-6

encapsulation, GRE tunnels, 1-2

equal-cost multipath, NAT support, 2-33

Error Authority parameter (RIPSO), 3-15, A-43

Error Label parameter (RIPSO), 3-15, A-43

error labels (RIPSO)
- defined, 3-3
- disabling use of, 3-15
- enabling use of, 3-15

ESH Configuration Timer parameter (OSI), 1-15

F

FTP
- address translations for, 2-5
- SDPT configuration considerations, 2-34

FTP port command, payload packet translation, 2-32

G

Generic Routing Encapsulation. *See* GRE

GRE
- overview, 1-2
- packet headers, 1-5
- Site Manager parameters, A-2
- tunnel, defined, 1-2
- *See also* tunnels (GRE)

gre command (BCC), 1-10

H

HTTP, address translations for, 2-5

I

ICMP support limitation for NAT, 2-39

IIH Hello Timer parameter (OSI), 1-15

IIH Hold Time Multiplier parameter (OSI), 1-15

Implicit Authority parameter (RIPSO), 3-13, A-40

Implicit Label parameter (RIPSO), 3-13, A-40

implicit labels (RIPSO)
- defined, 3-5
- supplying, 3-13

Implicit Level parameter (RIPSO), 3-13, A-41

Install Private Address parameter (NAT global), A-10

IP Address parameter (NAT)
- N-to-1, 2-114
- source address filter, 2-98, 2-102, A-28
- translation pool, 2-108, A-32

IP address, circuitless, using as GRE tunnel interface, 1-4

ip command (BCC), 1-12

IP Interface parameter (GRE), 1-11, A-3

IPsec support limitation for NAT, 2-34

ipx command (BCC), 1-13

ISH Hello Timer parameter (OSI), 1-15

ISH Hold Time Multiplier parameter (OSI), 1-15

ISP mode support limitation for NAT, 2-33

L

L1 Default Metric parameter (OSI), 1-15

L1 Designated Router Priority parameter (OSI), 1-15

L2 Default Metric parameter (OSI), 1-15

L2 Designated Router Priority parameter (OSI), 1-15

local tunnel end point (GRE)
- adding protocol to, 1-12
- deleting, 1-27
- disabling, 1-21
- reenabling, 1-21

Log Mask parameter (NAT global), 2-70, A-9

logical-ip-address command (BCC), 1-18

logical-ipx-address command (BCC), 1-18

log-mask command (BCC), 2-69

M

mapping aging (NAT)
- timeout value for dynamic translations, 2-72
- timer, enabling/disabling for dynamic translations, 2-71

Mapping Aging parameter (NAT global), 2-72, A-9

Mapping Timeout parameter (NAT global), 2-73, A-10

Maximum Level parameter (RIPSO), 3-10, A-37

May In Authority parameter (RIPSO), 3-12, A-39

May Out Authority parameter (RIPSO), 3-11, A-38

messages (NAT), logging, 2-69

Minimum Level parameter (RIPSO), 3-10, A-37

multidomain NAT. *See* bidirectional NAT

Must In Authority parameter (RIPSO), 3-12, A-39

Must Out Authority parameter (RIPSO), 3-11, A-38

N

NAT
- address translations, checking, B-10
- BGP support limitation, 2-33
- bidirectional
  - advantages, 2-7
  - BGP support limitation, 2-33
  - defined, 2-7
  - DNS client requirement, 2-8
  - DNS proxy considerations, 2-87
  - DNS proxy requirement for dynamic, 2-8
  - DNS server requirement, 2-8
  - dynamic translation (walkthrough), 2-50, B-3
  - ECMP mode support limitation, 2-33
  - how dynamic translation works, 2-28
  - how static translation works, 2-26
  - IPsec support limitation, 2-34
  - OSPF support limitation, 2-33
  - public router interfaces, 2-32
  - requirements, 2-7
  - static mapping, 2-84
  - three domains, 2-29
  - two domains, 2-28

checking translations with show commands, B-10

deleting from router, 2-79

domain
- defined, 2-2
- number of router interfaces to each, 2-32
- show nat domains command (BCC), B-11

domain name
- bidirectional, 2-8
- requirements, 2-52
- show nat domains command (BCC), B-11
- unidirectional, special, 2-3

dynamic translations
- adding a source address filter, 2-97
- adding a translation pool, 2-106
- address range considerations, 2-11
- address range for source address filter, 2-98
- bidirectional (walkthrough), 2-50, B-3
- comparison of unidirectional and bidirectional, 2-12
- configuring, 2-95
- defined, 2-10
- deleting a source address filter, 2-105
- deleting a translation pool, 2-111
- disabling a source address filter, 2-103
- disabling a translation pool, 2-109
- DNS proxy requirement, 2-8
- enabling a source address filter, 2-103
- enabling a translation pool, 2-109
- how bidirectional NAT works, 2-28
- how unidirectional NAT works, 2-15
- mapping aging, enabling timer, 2-71
- overview, 2-11
- port (N-to-1), 2-113

NAT *(continued)*
dynamic translations *(continued)*
reenabling a source address filter, 2-103
reenabling a translation pool, 2-109
source address filter, deleting, 2-105
timeout value, 2-72
translation pool, deleting, 2-111
unidirectional (walkthrough), 2-40
ECMP support limitation, 2-33
enabling on the router, 2-66
ICMP support, 2-39
IP forwarding requirements, 2-33
IPsec support limitation, 2-34
ISP mode support limitation, 2-33
log mask, configuring, 2-69
mappings, show nat command (BCC), B-12
messages, logging, 2-69
monitoring translations with show commands, B-10
N-to-1 translation
aging of translation table entries, 2-5
compared with SDPT, 2-5
configuring, 2-113
defined, 2-5
direction of translation, 2-5
dynamic port, 2-113
how N-to-1 works, 2-23
ICMP support limitation, 2-39
packet types, applicable, 2-5
when to use, 2-6
number of router interfaces per domain, 2-32
OSPF support limitation, 2-33
overview, 2-2
port translation
sample N-to-1 configuration, 2-23
sample SDPT configuration, 2-21
private address, defined, 2-3
public address, defined, 2-3
RIP for IP forwarding requirement, 2-33
router interfaces
adding NAT to, 2-74
private, defined, 2-32
public, defined, 2-32
show nat interfaces command (BCC), B-7
SDPT
address mapping, 2-89
aging of translation table entries, 2-5
compared with N-to-1, 2-5
defined, 2-5
direction of translation, 2-5
FTP configuration considerations, 2-34
how SDPT works, 2-20
packet types, applicable, 2-5
port mapping, 2-89
TFTP configuration considerations, 2-34
when to use, 2-6
show nat commands (BCC), 2-13, B-10
domains, B-11
filters, B-8
interfaces, B-7
mappings, B-12
pools, B-8
summary, B-10
show nat commands (Technician Interface), B-10
translations, B-13
Site Manager parameters, A-7
soloist slot, configuring, 2-67
source address filter
adding, 2-97
address range considerations, 2-11
address range, specifying, 2-98
defined, 2-11
deleting, 2-105
disabling, 2-103
enabling, 2-103
more than one in a domain, 2-11
reenabling, 2-103
show nat filters command (BCC), B-8
translation pool to use with, 2-98
translation precedence for multiple, 2-35
static translations
bidirectional address mapping, 2-84
configuring, 2-80
defined, 2-10
deleting address mapping, 2-93
how bidirectional works, 2-26
how N-to-1 address translation works, 2-23
how SDPT works, 2-20
how unidirectional works, 2-14
overview, 2-10
unidirectional address mapping, 2-81
TCP applications, translating addresses for, 2-5
translation pool
adding, 2-106
address range considerations, 2-11
defined, 2-11
deleting, 2-111

NAT *(continued)*
translation pool *(continued)*
disabling, 2-109
enabling, 2-109
more than one in a domain, 2-11
pairing with source address filter, 2-98
reenabling, 2-109
show nat pools command (BCC), B-8
translation precedence among different types, 2-35
translation table, 2-15
translations
checking, B-10
show nat command (Technician Interface), B-13
UDP applications, translating addresses for, 2-5
unidirectional
advantages, 2-3
defined, 2-3
destination domain name, special, 2-3
domain name private, 2-3
domain name public, 2-3
dynamic translation (walkthrough), 2-40
how dynamic translation works, 2-15
how N-to-1 translation works, 2-23
how SDPT works, 2-20
how static translation works, 2-14
N-to-1 translation, 2-5
private interface, 2-32
public interface, 2-32
requirements, 2-4
SDPT, 2-5
source domain name, special, 2-3
static mapping, 2-81

nat command (BCC), 2-74

Network Address Translation. *See* NAT

Nto1 Address parameter (NAT), source address filter, 2-102, 2-114, A-26, A-30

n-to-1 command (BCC), 2-113

N-to-1 translation (NAT)
aging of translation table entries, 2-5
compared with SDPT, 2-5
configuring, 2-113
defined, 2-5
direction of translation, 2-5
dynamic port, 2-113
how N-to-1 works, 2-23
ICMP support limitation, 2-39
packet types, applicable, 2-5
when to use, 2-6

O

OSPF support limitation for NAT, 2-33

P

port translation (NAT)
configuring N-to-1 translation, 2-113
configuring SDPT, 2-89
dynamic (N-to-1), 2-5
sample N-to-1 configuration, 2-23
SDPT sample, 2-21
static (SDPT), 2-5, 2-89

Prefix Length parameter (NAT)
N-to-1, 2-114
source address filter, 2-98, 2-102, A-28
translation pool, 2-108, A-33

private address (NAT), defined, 2-3

Private Address parameter (NAT)
SDPT, 2-91, A-20
static address mapping, A-13
static bidirectional, 2-88, A-17
static unidirectional, 2-83, A-22

Private Port parameter (NAT)
SDPT, 2-91, A-21
static mapping, A-13

product support, xix

Protocol parameter (NAT SDPT), 2-91, A-22

protocols, encapsulated in GRE tunnels
adding, 1-12
deleting, 1-24
disabling, 1-22
listed, 1-2
reenabling, 1-22

public address (NAT), defined, 2-3

Public Address parameter (NAT)
SDPT, 2-91, A-21
static bidirectional, 2-88, A-18
static unidirectional, 2-83, A-22

Public Port parameter (NAT SDPT), 2-91, A-21

publications
hard copy, xix
related, xviii

R

Redirect Enable/Disable parameter (OSI), 1-15
reenabling
GRE
remote tunnel end point, 1-25
tunnel, 1-21
tunnel protocol (IP, IPX, or OSI), 1-22
NAT
on an interface, 2-77
source address filter, 2-103
static address mapping, 2-92
translation pool, 2-109
Remote Logical IP Address parameter (GRE), 1-19, A-6
Remote Logical IPX Address parameter (GRE), 1-19, A-6
Remote Physical IP Address parameter (GRE), 1-19, 1-20, A-6
remote tunnel end point (GRE)
configuring, 1-16
configuring a remote logical interface (BCC)
IP protocol, 1-18
IPX protocol, 1-18
configuring a remote logical interface (Site Manager)
IP protocol, 1-19
IPX protocol, 1-19
OSI protocol, 1-20
configuring a remote physical interface
BCC, 1-17
Site Manager, 1-19
defined, 1-16
deleting, 1-26
disabling, 1-25
logical interface, 1-16
physical interface, 1-16
reenabling, 1-25
remote-endpoint command (BCC), 1-17
Require In Security parameter (RIPSO), 3-9, A-36
Require Out Security parameter (RIPSO), 3-8, A-36
requirements
for bidirectional NAT, 2-7
for unidirectional NAT, 2-4
Revised IP Security Option. *See* RIPSO
RIP for IP forwarding (NAT), 2-4
RIPSO
default labels
defined, 3-5
enabling or disabling use of, 3-14
disabling on an interface, 3-6
enabling on an interface, 3-6
error labels
defined, 3-3
disabling use of, 3-15
enabling use of, 3-15
example of, 3-16
implicit labels
defined, 3-5
supplying, 3-13
overview, 3-2
security labels
format, 3-3
inbound datagram types for, specifying, 3-9
outbound datagram types for, specifying, 3-8
security levels for IP datagrams, 3-10
Site Manager parameters, A-34
stripping security options from datagrams, 3-7
unlabeled IP datagrams, 3-5
Router ID parameter (OSI), 1-15
Routing Level parameter (OSI), 1-15
routing loops, in GRE tunnels, avoiding, 1-7

S

SDPT (NAT)
address mapping, 2-89
aging of translation table entries, 2-5
compared with N-to-1, 2-5
defined, 2-5
direction of translation, 2-5
FTP configuration considerations, 2-34
how SDPT works, 2-20
packet types, applicable, 2-5
port mapping, 2-89
TFTP configuration considerations, 2-34
when to use, 2-6

security classification (RIPSO), 3-4
security labels (RIPSO)
format, 3-3
specifying inbound datagram types that require, 3-9
specifying outbound datagram types that require, 3-8
security levels for IP datagrams (RIPSO), 3-10
security stripping options (RIPSO), specifying datagram types for, 3-7
show nat commands (BCC), 2-13, B-10
domains, B-11
filters, B-8
interfaces, B-7
mappings, B-12
pools, B-8
summary, B-10
show nat commands (Technician Interface), B-10
translations, B-13
slot-mask command (BCC), 2-67
soloist slot (NAT), configuring, 2-67
Soloist Slot Mask parameter (NAT global), 2-68, A-8
source address filter (NAT)
adding, 2-97
address range considerations, 2-11
address range, specifying, 2-98
defined, 2-11
deleting, 2-105
disabling, 2-103
enabling, 2-103
more than one in a domain, 2-11
reenabling, 2-103
translation pool to use with, 2-98
translation precedence for multiple, 2-35
Source Domain parameter (NAT)
static address translation, A-14
static bidirectional, 2-88, A-18
src-filter command (BCC), 2-100
state command (BCC)
GRE
remote tunnel end point, 1-25
tunnel, 1-21
tunnel protocol, 1-22
NAT
global, 2-66
interface, 2-77
source address filter, 2-103
static address mapping, 2-92
translation pool, 2-109
Static Nexthop parameter (NAT)
source address filter, 2-99, 2-102, A-27, A-30
static bidirectional, 2-88, A-19
static mapping, A-15
static unidirectional, 2-83, A-23
static routes
configuring for GRE tunnels, 1-7
IP forwarding requirement for NAT, 2-33
used with GRE tunnels, 1-8
static translations (NAT)
bidirectional address mapping, 2-84
configuring, 2-80
defined, 2-10
deleting address mapping, 2-93
how bidirectional works, 2-26
how N-to-1 address translation works, 2-23
how SDPT works, 2-20
how unidirectional works, 2-14
overview, 2-10
unidirectional address mapping, 2-81
static-map command (BCC)
bidirectional NAT, 2-86
unidirectional NAT, 2-82
static-sdpt command (BCC), 2-89
Strip Security parameter (RIPSO), 3-7, A-35
support, Nortel Networks, xix

T

TCP applications, address translations for, 2-5
technical publications, xix
technical support, xix
Telnet, address translations for, 2-5
text conventions, xvi
TFTP
address translations for, 2-5
SDPT configuration considerations, 2-34

timeout (NAT)
aging, enabling/disabling, 2-71
value, configuring for dynamic translations, 2-72
timeout command (BCC), 2-71
timeout-max command (BCC), 2-73
translation pool (NAT)
adding, 2-106
address range considerations, 2-11
defined, 2-11
deleting, 2-111
disabling, 2-109
enabling, 2-109
more than one in a domain, 2-11
pairing with source address filter, 2-98
reenabling, 2-109
Translation Pool Selector parameter (NAT), 2-98, 2-102, A-26, A-29
translation precedence (NAT), 2-35
translations
checking network address, B-10
dynamic. *See* dynamic translations (NAT)
network address (NAT), 2-1
static. *See* static translations (NAT)
trans-pool command (BCC), 2-107
Tunnel Name parameter (GRE), 1-11, A-3
tunnels (GRE)
adding protocol to local tunnel end point, 1-12
definition, 1-2
deleting, 1-27
end points
configuring local, 1-10
configuring remote, 1-16
maximum, 1-9
limitations, 1-2, 1-7
logical address, defined, 1-3
maximum number per router, 1-9
modifying configured, 1-21
physical address, defined, 1-3
requirements for encapsulating IP, 1-7
routing loops, avoiding, 1-7
See also local tunnel end point (GRE), remote tunnel end point (GRE)
tunnels command (BCC), 1-10

U

UDP applications, translations for, 2-5
unidirectional NAT
advantages, 2-3
defined, 2-3
destination domain name, special, 2-3
domain name private, 2-3
domain name public, 2-3
dynamic translation (walkthrough), 2-40
how dynamic translation works, 2-15
how N-to-1 translation works, 2-23
how SDPT works, 2-20
how static translation works, 2-14
N-to-1 translation, 2-5
private interface, 2-32
public interface, 2-32
requirements, 2-4
SDPT, 2-5
source domain name, special, 2-3
static mapping, 2-81
unlabeled IP datagrams (RIPSO), 3-5
Unnumbered CCT Name parameter (NAT)
source address filter, 2-99, 2-102, A-27, A-31
static address mapping, A-16
static bidirectional, A-20
static unidirectional, 2-83, A-23

V

VPN (virtual private network), 1-2

X

X.25, BFE support
packet-level parameter settings, 4-6
service-level parameter settings, 4-8